МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ**

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “ ДОСЛІДЖЕННЯ ВПЛИВУ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ НА ОРГАНІЗАЦІЙНУ КІБЕРБЕЗПЕКУ ТА СТВОРЕННЯ МЕТОДІВ ПРОТИДІЇ ”

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Роман ІВАЩЕНКО
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав(ла): здобувач вищої освіти гр. УБД-42

Роман ІВАЩЕНКО
Ім’я, ПРІЗВИЩЕ

Керівник: Юрій ЩАВІНСЬКИЙ
к.т.н., доцент Ім’я, ПРІЗВИЩЕ

Рецензент: _____
Ім’я, ПРІЗВИЩЕ

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут захисту інформації

Кафедра управління інформаційною та кібернетичною безпекою

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УІКБ
_____ Світлана ЛЕГОМІНОВА
“____”_____2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Іващенку Роману Сергійовичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “ Дослідження впливу соціальної інженерії на організаційну кібербезпеку та створення методів протидії ”,
керівник кваліфікаційної роботи ЩАВІНСЬКИЙ Юрій, к.т.н., доцент,
(ІПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологійвід “27“ *лютого 2024* р. № *36*.

2. Строк подання кваліфікаційної роботи “20” травня 2024р.

3. Вихідні дані до кваліфікаційної роботи: *наукова та технічна література, міжнародні стандарти, методи та засоби соціальної інженерії, методи протидії соціальній інженерії*

4. Перелік питань, які мають бути розроблені:
   4.1. Аналіз теоретичних основ, методів та технік соціальної інженерії.
   4.2. Аналіз впливу соціальної інженерії на організаційну кібербезпеку.
   4.3. Розроблення методів протидії соціальній інженерії.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “11“ березня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2024	
2.	Збір та аналіз літератури.	29.03.2024	
3.	Аналіз теоретичних основ, методів та технік соціальної інженерії	08.04.2024	
4.	Аналіз впливу соціальної інженерії на організаційну кібербезпеку.	22.04.2024	
5.	Розроблення методів протидії соціальній інженерії	08.05.2024	
6.	Формулювання висновків за результатами проведеного дослідження.	20.05.2024	
7.	Оформлення роботи.	22.05.2024	
8.	Оформлення презентації.	03.06.2024	
9.	Отримання рецензії на роботу.	03.06.2024	
10.	Захист в ДЕК.	__.06.2024	

Здобувач вищої освіти _____ Роман ІВАЩЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Юрій ЩАВІНСЬКИЙ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня бакалавра

Направляється здобувач Іващенко Р.С. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: “ Дослідження впливу соціальної інженерії на організаційну кібербезпеку та створення методів протидії ”

Кваліфікаційна робота і рецензія додаються.

Директор ННІЗІ _____ Віталій САВЧЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач ІВАЩЕНКО Роман у кваліфікаційній роботі проаналізував методи та техніки соціальної інженерії, дослідив вплив соціальної інженерії на організаційну кібербезпеку, розробив метод протидії соціальній інженерії та оцінив його ефективність і відпрацював рекомендації для практичного застосування.

ІВАЩЕНКО Роман показав розуміння проблеми дослідження та бачення основних теоретичних і практичних напрямів її вирішення, довів здатність самостійного застосування методів наукового дослідження, проявив себе як організований, відповідальний виконавець. Результати дослідження апробовані на науково-практичні конференції.

Все це дозволяє оцінити кваліфікаційну роботу здобувача ІВАЩЕНКА Романа на оцінку “добре” та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Юрій ЩАВІНСЬКИЙ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

“____“_____2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Іващенко Р.С.. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри
управління інформаційною
та кібернетичною безпекою _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти ІВАЩЕНКО Романа
на тему “ Дослідження впливу соціальної інженерії на організаційну кібербезпеку та створення методів протидії ”

Актуальність. У сучасному світі кіберзагрози стають все більш поширеними і складними. Соціальна інженерія є однією з найбільш ефективних та часто використовуваних методів атак, що базуються на маніпулюванні людським фактором. З розвитком нових технологій виникають нові вектори атак, які можуть бути експлуатовані через соціальну інженерію. Це підвищує необхідність досліджень і розробки адаптивних методів протидії. Сучасні підходи до кібербезпеки потребують комплексного підходу, що включає як технічні, так і організаційні заходи. Це робить дослідження впливу соціальної інженерії надзвичайно актуальним. Вивчення впливу соціальної інженерії та розробка методів протидії допоможе створити більш стійку систему кібербезпеки для організацій.

Позитивні сторони.

1. У роботі зроблений аналіз впливу соціальної інженерії на організаційну кібербезпеку, за результатами аналізу виявлена потреба в удосконаленні методів протидії соціальній інженерії, вибрані доцільні технології та інструменти для розроблення програмного забезпечення з метою удосконалення сучасних методів протидії впливу соціальної інженерії на організаційну безпеку та підготовлені пропозиції.

2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено відповідно до плану, зроблено логічні висновки. Ключові положення роботи представлено у вигляді рисунків.

3. Автор опрацював значну джерельну базу наукових публікацій, в тому числі англомовних.

4. За результатами дослідження запропоновано рекомендації щодо застосування методу протидії впливу соціальної інженерії на організаційну безпеку.

Недоліки. Доцільно було б приділити більше уваги вивченню і класифікації програмних інструментів для оцінки ефективності розробленого методу протидії впливу соціальній інженерії.

Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки “добре”, а здобувач ІВАЩЕНКО Роман заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент: _____ _____ _____
науковий ступінь вчене звання *підпис* Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню впливу соціальної інженерії на організаційну кібербезпеку та створенню методів протидії соціальній інженерії. Робота складається зі вступу, трьох розділів, що містять 15 рисунків, 1 таблиця, висновків і списку використаних джерел із 35 найменувань та додатків. Загальний обсяг роботи становить 65 аркуші, з яких 11 аркушів займають список використаних джерел та додатки.

Метою роботи є розробка методів протидії впливу соціальної інженерії на організаційну кібербезпеку.

Об'єкт дослідження є вплив соціальної інженерії на організаційну кібербезпеку.

Предмет дослідження – методи протидії впливу соціальної інженерії на організаційну кібербезпеку.

Методи дослідження: аналіз при огляді наукових джерел та методів дослідження; мета-аналіз і контент-аналіз наукових публікацій, аналіз журналів та логів для виявлення підозрілих активностей та інцидентів, математичне моделювання при розробленні програмного забезпечення.

Як результат, у роботі було проаналізовано сучасні методи впливу соціальної інженерії на організаційну кібербезпеку та виявлена потреба в їх удосконаленні. Розроблено удосконалений метод протидії впливу соціальної інженерії на організаційну кібербезпеку за рахунок програмного забезпечення та відпрацьовані пропозиції з його застосування.

Галузь застосування. Розроблений метод протидії впливу соціальної інженерії на організаційну кібербезпеку може бути використаний для організацій та підприємств з урахуванням їх особливостей.

Ключові слова: ОРГАНІЗАЦІЙНА КІБЕРБЕЗПЕКА, СОЦІАЛЬНА ІНЖЕНЕРІЯ, МЕТОДИ ПРОТИДІЇ,

ABSTRACT

The qualification work is dedicated to studying the impact of social engineering on organizational cybersecurity and developing methods to counteract social engineering. The thesis consists of an introduction, three chapters containing 15 figures, 1 table, conclusions, a list of references with 35 sources, and appendices. The total volume of the work is 65 pages, of which 11 pages are occupied by the list of references and appendices.

The purpose of the study is to develop methods to counteract the impact of social engineering on organizational cybersecurity.

The object of the study is the impact of social engineering on organizational cybersecurity.

The subject of the study is the methods to counteract the impact of social engineering on organizational cybersecurity.

Research methods: analysis in reviewing scientific sources and research methods; meta-analysis and content analysis of scientific publications, analysis of logs and journals to detect suspicious activities and incidents, mathematical modeling in software development.

As a result, the thesis analyzed modern methods of social engineering impact on organizational cybersecurity and identified the need for their improvement. An enhanced method to counteract the impact of social engineering on organizational cybersecurity through software was developed, and proposals for its application were refined.

Field of application. The developed method to counteract the impact of social engineering on organizational cybersecurity can be used by organizations and enterprises, taking into account their specific features.

Keywords: ORGANIZATIONAL CYBERSECURITY, SOCIAL ENGINEERING, COUNTERMEASURES

ЗМІСТ

ВСТУП

Актуальність теми. Сучасні організації все частіше стають об'єктами кібератак, спрямованих на компрометацію їхніх інформаційних систем та викрадення конфіденційних даних. Кількість інцидентів кібербезпеки зростає, і соціальна інженерія є однією з основних технік, що використовуються зловмисниками для здійснення таких атак. Згідно з дослідженнями, понад 90% успішних кібератак починаються саме з використання методів соціальної інженерії. Вивчення впливу соціальної інженерії на організаційну кібербезпеку та розробка методів протидії є вкрай важливими для забезпечення ефективного захисту інформаційних систем. Це допоможе організаціям зменшити ризики, пов'язані з кіберзагрозами, зберегти конфіденційність даних та відповідати сучасним регуляторним вимогам

Мета роботи полягає у дослідженні впливу соціальної інженерії на організаційну безпеку та розроблення методів протидії впливу соціальної інженерії на організаційну кібербезпеку.

Об'єктом дослідження є вплив соціальної інженерії на організаційну кібербезпеку.

Предмет дослідження – методи протидії впливу соціальної інженерії на організаційну кібербезпеку.

Для досягнення цієї мети в роботі необхідно виконати наступні завдання:

1. Здійснити аналіз теоретичних основ, методів та технік соціальної інженерії.

2. Проаналізувати вплив соціальної інженерії на організаційну кібербезпеку.

3. Розробити методи протидії соціальній інженерії.

Методи дослідження. Для вирінення завдань в роботі застосовані: аналіз при огляді наукових джерел та методів дослідження; мета-аналіз і контент-аналіз наукових публікацій, статей та доповідей; аналіз журналів та логів для виявлення підозрілих активностей та інцидентів, які можуть бути пов'язані з атаками

соціальної інженерії; аналіз інцидентів при дослідженні реальних випадків кібератак, пов'язаних із соціальною інженерією, для виявлення причин, методів та наслідків; моделювання при розробленні методів протидії соціальній інженерії.

Практичне значення одержаних результатів. Отримані результати можуть бути використані в організаціях та на підприємствах з урахуванням особливостей функціонування системи їх кібербезпеки. з метою підвищення рівня кібербезпеки компанії та зменшення можливих збитків.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 28 лютого 2024 року.

Розділ 1 ТЕОРЕТИЧНІ ОСНОВИ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ І ОРГАНЗАЦІЙНОЇ КІБЕРБЕЗПЕКИ

1.1. Поняття та сутність соціальної інженерії

За останні роки соціальні мережі стали не тільки популярними для особистого використання, але і для робочих цілей. Це також створює нові можливості для соціальної інженерії, оскільки атакуючі можуть здійснювати дослідження про потенційні цілі або використовувати існуючі взаємодії для атаки

Соціальна інженерія вважається однією з найбільш значущих сучасних загроз інформаційній безпеці. Незважаючи на її повсюдне використання серед онлайн-кримінальних субкультур і практиків безпеки, не існує єдиної узгодженої концептуалізації «соціальної інженерії».

У ландшафті кібербезпеки, що постійно розвивається, соціальна інженерія постає як витончена форма маніпуляції, що використовує найбільш непередбачуваний елемент систем безпеки: людський фактор. На відміну від традиційних кібератак, спрямованих на усунення вразливостей системи за допомогою технічних засобів, атаки соціальної інженерії зосереджені на маніпулюванні людьми для добровільної компрометації протоколів безпеки, розкриття конфіденційної інформації або надання несанкціонованого доступу.

Науковці у своїх роботах дають декілька визначень соціальної інженерії.

Соціальна інженерія – це наука, що вивчає людську поведінку та фактори, які на неї впливають. Наприклад: вивчення середовища, в якому жив вбивця, допоможе зрозуміти його систему цінностей. Ця інформація надасть можливість розробити соціальну структуру, в якій будуть формуватись інші системи цінностей, у яких насамперед буде цінуватись людське життя та індивідуальність [1].

Соціальна інженерія – це кіберзагроза, яка використовує людську психологію, а не використовує технічні вразливості. Це включає в себе обманну

тактику, щоб змусити людей порушити нормальні процедури безпеки, що часто призводить до несанкціонованого доступу до систем, крадіжки даних або фінансового шахрайства [2] .

Соціальна інженерія визначається як використання соціальних маскувань, культурних хитрощів і психологічних прийомів, щоб змусити користувачів комп'ютерів допомогти хакерам у незаконному вторгненні або використанні комп'ютерних систем і мереж [3-5].

У контексті інформаційної безпеки соціальна інженерія визначається як зловмисна діяльність, спричинена кіберзлочинцями за допомогою взаємодії з людьми. В основному це техніка психологічної маніпуляції, яка використовує людську помилку для отримання приватної інформації. У дослідженні [6] використовувалися алгоритми машинного навчання, щоб передбачити сприйнятливість людей до атак соціальної інженерії. Учасникам дослідження були представлені змодельовані сценарії, і їх попросили визначити, чи є кожен сценарій атакою соціальної інженерії чи ні. Різні види атак, пов'язаних з різними галузями, були інтегровані в симуляції соціальної інженерії. Для кожного учасника відповідно до їхніх відповідей розраховувалися різні типи балів соціальної інженерії. Окрім симуляцій, учасники заповнювали анкети, пов'язані з демографічними показниками, використанням технологій та особистісними рисами. Всі зібрані дані були використані при побудові моделей прогнозної класифікації та регресійного машинного навчання. За допомогою регресійних і класифікаційних моделей аналіз дослідження був спрямований на проактивне прогнозування рівнів ризику соціальної інженерії індивідів і класифікацію їх на різні групи ризику з точки зору різних типів атак. дослідження показало, що можна заздалегідь визначити рівні ризику соціальної інженерії індивідів. Цей важливий висновок означає, що можливим нападам можна запобігти, підвищивши обізнаність до того, як напад відбудеться. У рамках цього дослідження також було розроблено мобільний додаток для виявлення ризиків соціальної інженерії, щоб дати практикам і політикам уявлення про те, які системи можуть бути розроблені для визначення рівнів ризику окремих осіб, а

потім для інформування їх про різні атаки.

Згідно з Оксфордським словником англійської мови, термін «соціальна інженерія» має два різних значення.

По-перше, це «використання централізованого планування у спробі керувати соціальними змінами та регулювати майбутній розвиток і поведінку суспільства».

По-друге, це «використання обману з метою спонукання особи до розголошення приватної інформації або, зокрема, для несанкціонованого доступу до комп'ютерної системи чи мережі».

У той час як обидва визначення передбачають, що один або кілька індивідів викликають поведінку інших, перше явно знаходить своє застосування в сфері політичного та економічного управління, тоді як друге знаходить своє місце унікально в області кіберпростору. Науковці стверджують, що використання цього терміну в обох сферах залишається концептуально та семантично взаємопов'язаним [7] . Більше того, незнання цього взаємозв'язку продовжує перешкоджати нашій здатності виявляти та відбивати атаки соціальної інженерії в кіберпросторі.

1.2 Історія розвитку соціальної інженерії

Концептуальна історія починається в дев'ятнадцятому столітті в працях економістів. Аналіз наукових статей показує поширення цієї концепції протягом початку-середини XX століття в соціальних науках і за їх межами. Потім простежується міграція концепції в кібербезпеку протягом 1960–1980-х років, використовуючи як наукові публікації, так і мемуарні розповіді, включаючи інтерв'ю з активними учасниками хакерської спільноти. Нарешті, він розкриває концептуальний масив сучасних конотацій через аналіз 134 визначень терміну, знайдених в академічних статтях, написаних про кібербезпеку з 1990 по 2017 рік. Але соціальна інженерія має коріння, що сягають давнини, коли люди

використовували обман і маніпуляції для досягнення своїх цілей. Один з найбільш відомих прикладів ранньої соціальної інженерії - це історія про Троянського коня з давньогрецької міфології.

Троянський кінь: греки побудували великий дерев'яний кінь і залишили його перед воротами Трої як "подарунок". Троянці прийняли кінь всередину міста, вважаючи, що це знак капітуляції греків. Однак, всередині коня ховалися грецькі солдати, які вночі вийшли з нього і відкрили ворота міста для своєї армії, що призвело до падіння Трої. Цей приклад показує, як обман і маніпуляція можуть бути використані для досягнення стратегічних цілей.

З розвитком технологій на початку XX століття, зокрема телефону, соціальні інженери отримали нові можливості для шахрайства. Шахраї використовували телефон для видавання себе за представників банків або інших авторитетних організацій, щоб виманити у людей конфіденційну інформацію, таку як банківські реквізити або особисті дані. Цей метод став прообразом сучасних фішингових атак.

Холодна війна середина XX століття. Цей період холодної війни приніс новий етап розвитку соціальної інженерії, коли розвідслужби активно використовували маніпуляції для збору інформації. Агенти обох супердержав (США та СРСР) використовували техніки соціальної інженерії для проникнення в урядові структури і компанії супротивника. Вони видавали себе за дипломатів, журналістів або бізнесменів, щоб отримати доступ до секретних даних. Ці операції включали використання підроблених документів, легенд і створення складних історій для обману цілей.

Ера інформаційних технологій - кінець XX - початок XXI століття. З розвитком інтернету і комп'ютерних технологій соціальна інженерія набула нових форм. У 1990-х роках зловмисники почали використовувати електронну пошту для фішингових атак. Вони надсилали повідомлення, що виглядали як офіційні листи від банків або інших організацій, з метою виманити у користувачів їхні логіни, паролі або фінансові дані. Ці атаки стали дуже популярними через їхню простоту і ефективність.

У 2000-х роках почали з'являтися нові методи соціальної інженерії, такі як вішинг (телефонний фішинг) та смішинг (фішинг через SMS). Зловмисники використовували телефонні дзвінки та текстові повідомлення для того, щоб виманити у жертв конфіденційну інформацію.

Сучасний етап XXI століття. У сучасному світі соціальна інженерія продовжує розвиватися і адаптуватися до нових технологій та соціальних умов. З поширенням соціальних мереж зловмисники отримали нові можливості для збору інформації про своїх цілей. Вони можуть аналізувати профілі користувачів, їхні звички та коло спілкування, щоб створити більш переконливі атаки. Наприклад, зловмисники можуть видавати себе за друзів або колег жертви, щоб отримати доступ до конфіденційної інформації.

Deepfake технології, новітні технології, такі як штучний інтелект відкривають нові горизонти для соціальної інженерії. З їх допомогою можна створювати підроблені відео або аудіозаписи, які виглядають і звучать як реальні, що робить атаки ще більш переконливими.

Сучасні соціальні інженери часто націлені на великі компанії та організації. Вони використовують складні схеми, такі як spear phishing (цільовий фішинг) або бізнес-емейл компрометації (BEC), щоб отримати доступ до корпоративних ресурсів або викрасти великі суми грошей [8-9].

Соціальна інженерія, як метод маніпуляції людьми для отримання конфіденційної інформації або доступу до ресурсів, має довгу історію. Хоча термін "соціальна інженерія" з'явився відносно недавно, принципи цього явища використовувалися задовго до появи сучасних технологій. Розглянемо основні етапи розвитку соціальної інженерії, обґрунтовуючи кожен з них.

Таким чином, історія соціальної інженерії демонструє еволюцію людських маніпуляцій, які використовувалися для досягнення різних цілей протягом століть. Історія соціальної інженерії підкреслює, що це явище базується на глибокому розумінні людської природи і соціальних взаємодій. Соціальні інженери використовують психологічні принципи, такі як авторитет, дефіцит, соціальне підтвердження, симпатія, взаємність, звичка і емоційний вплив, щоб

маніпулювати людьми. Це вимагає від захисників постійного оновлення знань і методів захисту.

Соціальна інженерія має значний вплив на бізнес і суспільство в цілому. Атаки на компанії можуть призвести до втрати конфіденційної інформації, фінансових збитків та шкоди репутації. Для індивідів це може означати втрату особистих даних і фінансових коштів. Ефективний захист від соціальної інженерії вимагає підвищення обізнаності та навчання як на індивідуальному, так і на корпоративному рівні. Співробітники повинні бути навчені розпізнавати потенційні атаки і знати, як на них реагувати. Інтеграція сучасних технологій, таких як багатофакторна автентифікація, системи моніторингу та штучний інтелект для виявлення аномалій, є критично важливою для захисту від соціальних інженерів. Крім того, політики безпеки повинні бути постійно оновлюваними та враховувати нові загрози.

Соціальна інженерія буде продовжувати еволюціонувати разом з розвитком технологій. Майбутні загрози можуть включати використання біометричних даних, розширення використання штучного інтелекту для більш персоналізованих атак і застосування нових технологій, таких як блокчейн, для створення нових схем шахрайства. Важливо, щоб суспільство і бізнес були готові до цих змін, розуміючи історичний контекст і сучасні тенденції соціальної інженерії. Знання минулого і готовність до майбутнього є ключовими елементами ефективної стратегії захисту від маніпуляцій і шахрайства.

1.3 Суть і принципи організаційної кібербезпеки

Організаційна кібербезпека – це комплекс заходів, процедур, політик та технологій, спрямованих на захист інформаційних систем, мереж, програм та даних в межах організації від кіберзагроз (рис.1.1).

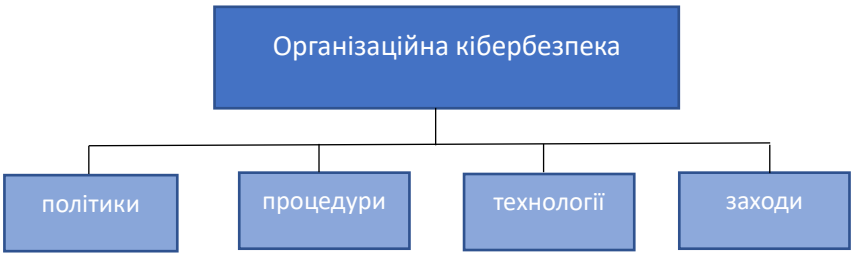

Рис. 1.1. Складові організаційної безпеки

Це включає не лише технічні аспекти, але й організаційні та людські фактори. Основні компоненти організаційної кібербезпеки включають:

1. Розробка та впровадження політик безпеки - визначення правил і стандартів, яких повинні дотримуватися всі працівники організації для забезпечення безпеки інформаційних ресурсів.

2. Процедури реагування на інциденти - планування дій на випадок кіберінцидентів, включаючи виявлення, реагування, відновлення та запобігання повторним атакам.

2. Заходи

Технічні:

мережева безпека - використання фаєрволів, систем виявлення вторгнень (IDS/IPS), VPN та інших технологій для захисту мережі;

шифрування - захист даних в процесі передачі та зберігання шляхом використання криптографічних методів;

антивірусне та антишпигунське програмне забезпечення - встановлення програм для виявлення та знешкодження шкідливого програмного забезпечення.

Організаційні

Управління доступом:

контроль доступу - впровадження системи, яка дозволяє доступ до інформаційних ресурсів лише авторизованим користувачам на основі ролей та обов'язків;

аутентифікація та авторизація - використання багатофакторної аутентифікації (MFA) для підтвердження ідентичності користувачів та контролю

доступу до ресурсів.

Навчання персоналу

підвищення обізнаності - регулярні тренінги для працівників щодо кібербезпеки, включаючи розпізнавання фішингових атак та інших методів соціальної інженерії;

симуляції кіберзагроз - проведення навчальних атак для перевірки готовності персоналу до реагування на реальні загрози.

Моніторинг та аудит:

безперервний моніторинг - використання систем для постійного моніторингу мереж та інформаційних систем на предмет підозрілої активності;

аудит безпеки - регулярні перевірки та оцінка відповідності політикам безпеки та стандартам.

Управління ризиками:

оцінка ризиків - визначення і оцінка можливих кіберзагроз і їхнього впливу на організацію;

мітигація ризиків - розробка та впровадження заходів для зменшення ризиків до прийнятного рівня.

Організаційна кібербезпека є невід'ємною частиною сучасної бізнес-стратегії, оскільки захист від кіберзагроз стає все більш важливим для збереження конфіденційності, цілісності та доступності даних, а також для підтримки довіри клієнтів і партнерів [10].

В Україні рішенням уряду від 29 грудня 2021 р. № 1426 [11] затверджена організаційно-технічна модель кіберзахисту (рис. 1.2), яка включає основні принципи організаційної кібербезпеки (рис. 1.3)

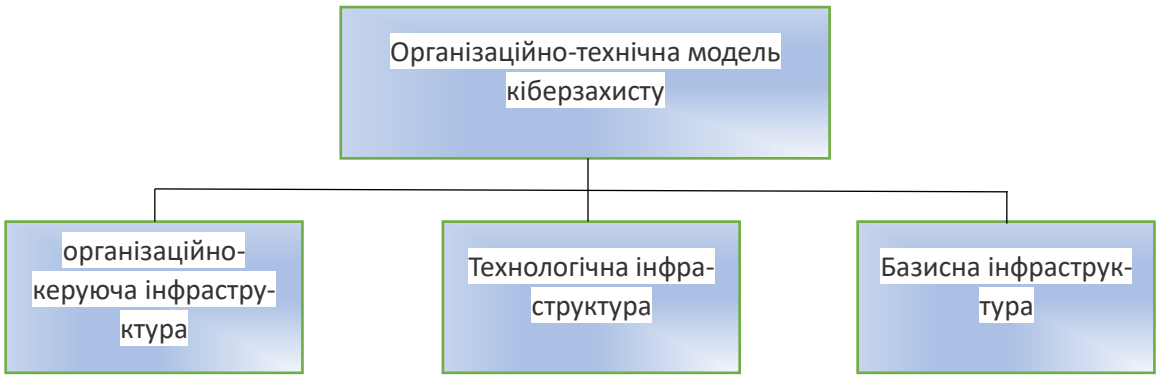

Рис. 1.2. Схема організаційно-технічної моделі кіберзахисту

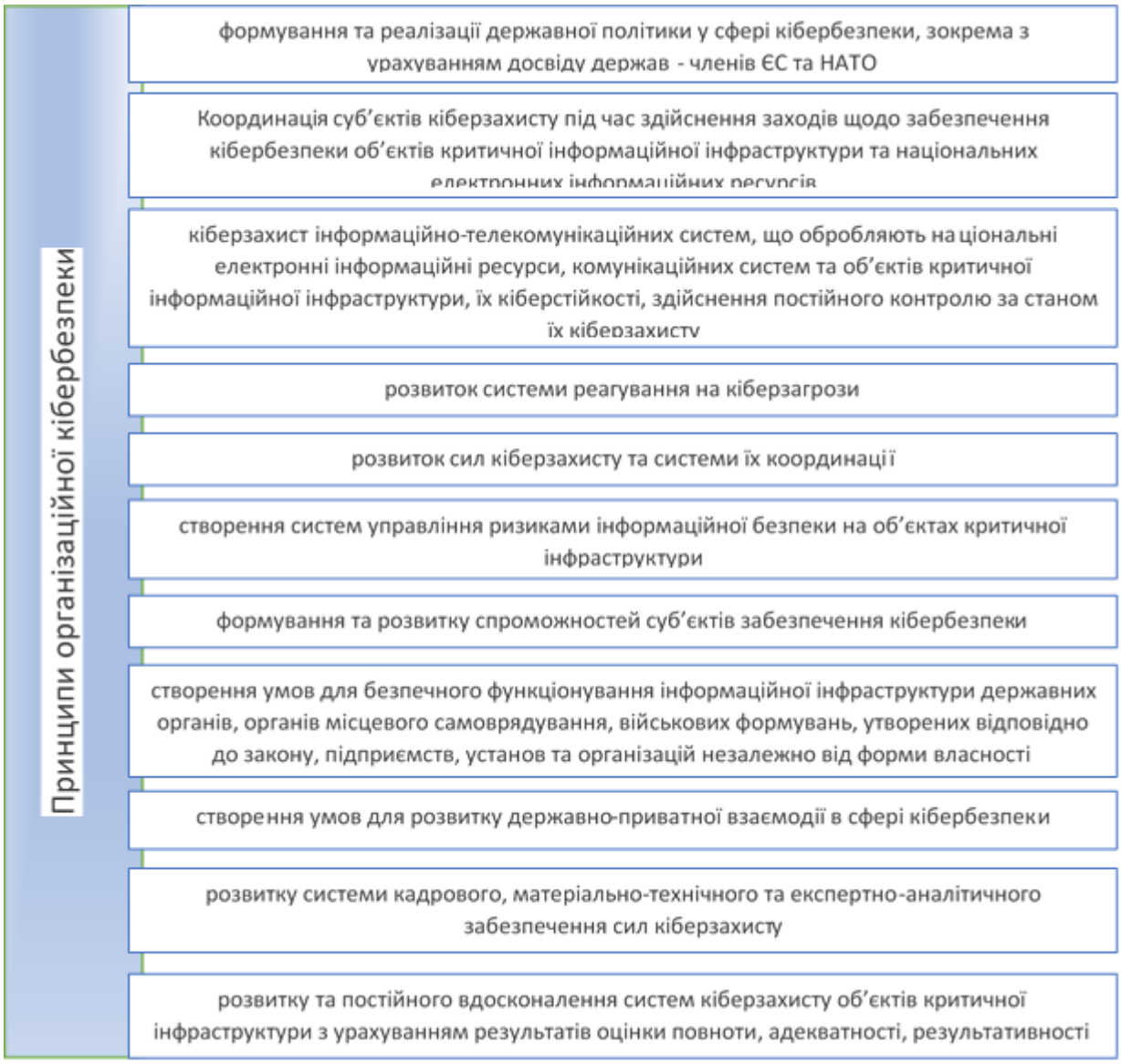

Рис. 1.3. Принципи організаційної кібербезпеки

Висновки до розділу 1

Розуміння соціальної інженерії має першорядне значення в цифрову епоху, коли інформація є як найціннішим активом, так і найбільш вразливою мішенню. Організації, які роблять перші кроки в напрямку кібербезпеки, швидко виявлять, що безсистемне, реактивне застосування засобів контролю не робить систему дуже ефективною. Майбутні загрози можуть включати використання біометричних даних, розширення використання штучного інтелекту для більш персоналізованих атак і застосування нових технологій, таких як блокчейн, для створення нових схем шахрайства

Проведений аналіз впливу соціальної інженерії на організаційну кібербезпеку виявив потребу в удосконаленні методів протидії соціальній інженерії

Розділ 2 АНАЛІЗ ВПЛИВУ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ НА ОРГАНІЗАЦІЙНУ КІБЕРБЕЗПЕКУ

2.1 Механізми впливу соціальної інженерії на організаційну кібербезпеку та сценарії кібератак

Соціальна інженерія стала серйозною загрозою у віртуальних спільнотах і є ефективним засобом атаки на інформаційні системи. Дослідники у своїх роботах уже протягом століття досліджують механізми впливу загроз соціальної інженерії на безпеку організацій та підприємств. В аспекті соціального впливу вони визначають [12] :

1) груповий вплив і конформізм$
2) нормативно-інформаційний вплив$
3) соціальний обмін і норма взаємності$
4) соціальна відповідальність та моральний обов'язок;
5) саморозкриття і побудова відносин взаєморозуміння;
6) дефіцит сприйняття цінності та збудження емоцій;
7) цейтнот і перевантаження думками;
8) довіра до джерела і підкорятися авторитету в переконанні;
9) відволікання уваги в переконаннях і маніпуляціях

Послуги, якими користуються сучасні інтелектуальні працівники, готують ґрунт для складних атак соціальної інженерії. Зростаюча тенденція до політики BYOD (bring your own device) та використання інструментів онлайн-спілкування та співпраці в приватному та діловому середовищі посилюють проблему. У глобально діючих компаніях команди більше не географічно розташовані разом, а укомплектовані персоналом з різних прошарків населення і навіть різних країн. Зниження особистої взаємодії в поєднанні з безліччю інструментів, що використовуються для комунікації (електронна пошта, миттєві повідомлення, Skype, Dropbox, LinkedIn, Lync тощо), створюють нові вектори атак для атак

соціальної інженерії. Нещодавні атаки на такі компанії, як New York Times і RSA Security, показали, що цілеспрямовані цільові фішингові атаки є ефективним, еволюційним кроком атак соціальної інженерії. У поєднанні з експлойтами нульового дня вони стають небезпечною зброєю, яку часто використовують просунуті постійні загрози.

Дослідження, проведені у працях [13-14] встановили шаблони та сценарії атак соціальної інженерії і сформулювали визначення як для соціальної інженерії («Мистецтво» впливу на людей з метою розкриття конфіденційної інформації відоме як соціальна інженерія), так для атаки соціальної інженерії. Крім того, автори запропонували онтологічну модель атаки соціальної інженерії. Вони визначили соціальну інженерію як «науку про використання соціальної взаємодії як засобу переконання індивіда чи організації виконати конкретний запит зловмисника, де або соціальна взаємодія, або переконання, або запит включають суб'єкта, пов'язаного з комп'ютером» [14].

Незважаючи на те, що онтологічна модель містить всі компоненти атаки соціальної інженерії, вона не в змозі відобразити часові дані, такі як потік і час. Через цей недолік автори розробили структуру атак соціальної інженерії, яка розширює цикл атак соціальної інженерії Кевіна Митника. Структура атаки, або цикли (рис. 2.1) соціальної інженерії зображує логічний хід атаки соціальної інженерії [14].

Ця структура відноситься до компонентів онтологічної моделі, але фокусується на потоці процесу – починаючи з моменту, коли зловмисник спочатку думає про отримання конфіденційної інформації від якоїсь цілі, до моменту досягнення успіху в досягненні мети отримання цієї інформації.
Кожен крок у рамках атаки соціальної інженерії було перевірено на реальних прикладах соціальної інженерії.

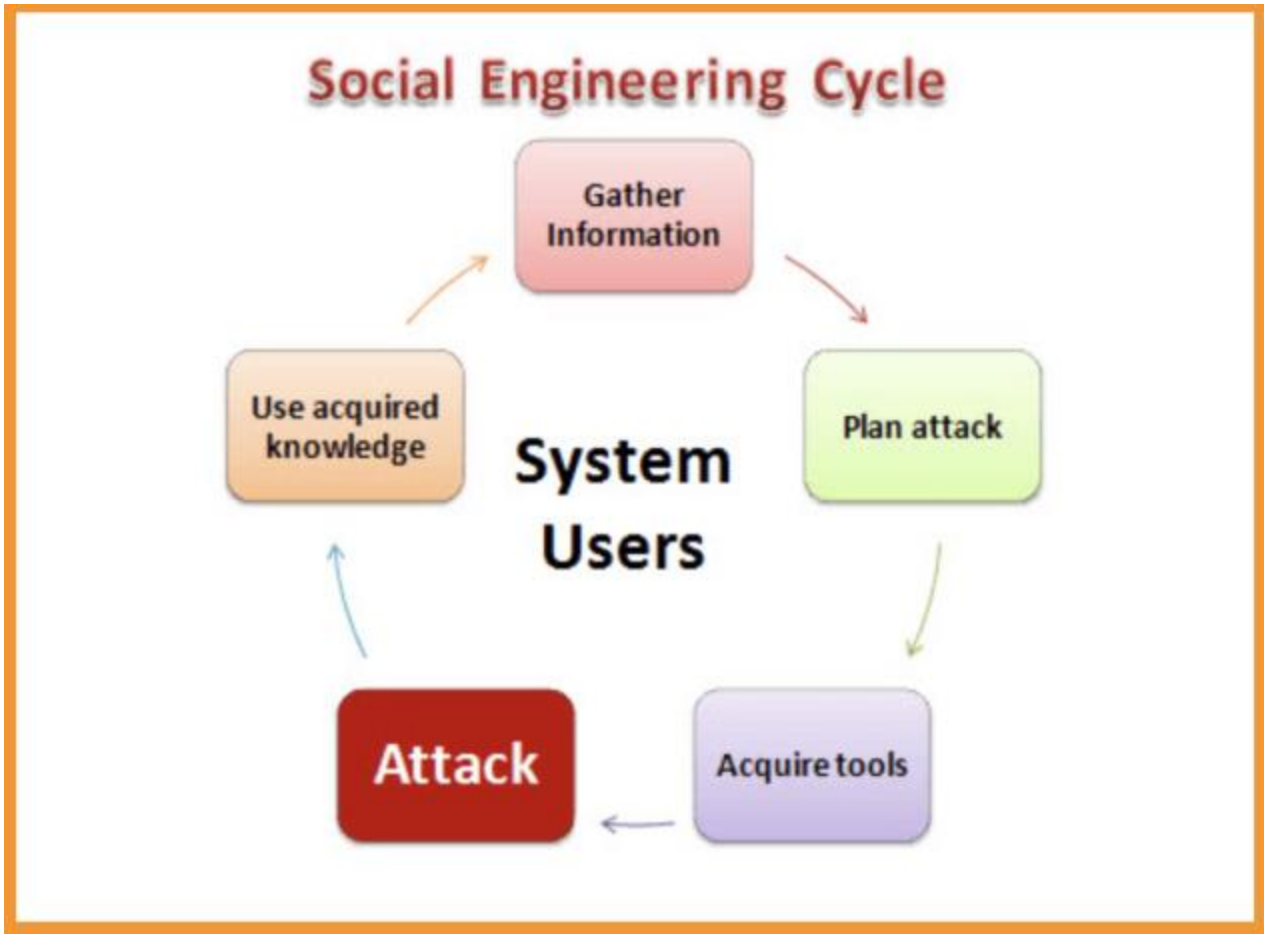

Рис. 2.1. Цикли атак соціальної інженерії

Проведені дослідження дозволили створити концептуальну модель атак соціальної інженерії (рис.2.2) яка забезпечує подальші пошуки науковців

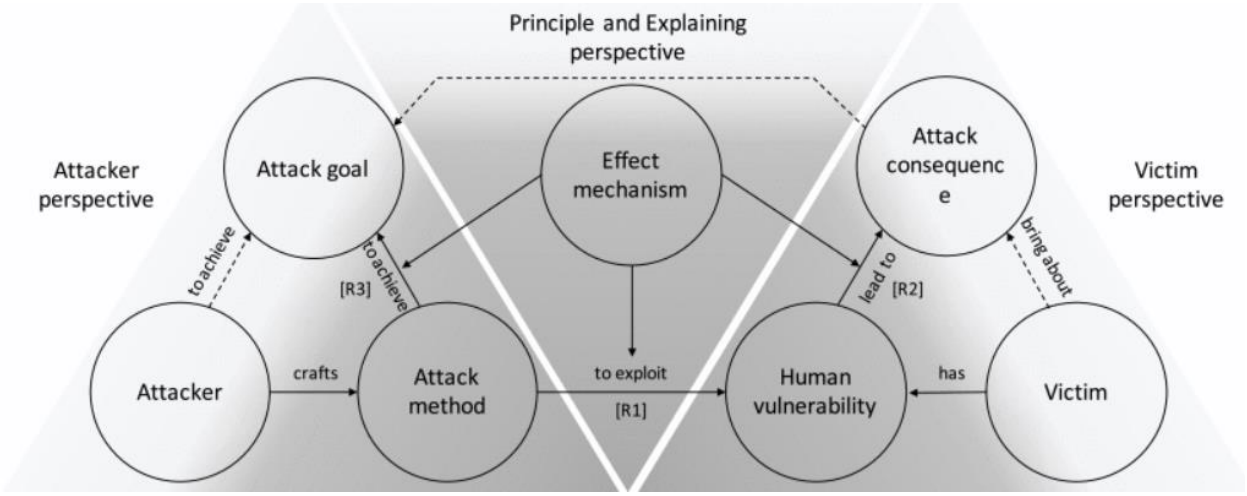

Рис.2.2. Концептуальна модель атак соціальної інженерії [12]

Разом з тим, дослідники виявили [3-5, 7-8], що кількість практичних прикладів соціальної інженерії в літературі обмежена, сучасна література, присвячена атакам соціальної інженерії, не відображає повного процесу атаки соціальної інженерії, і коли дослідники використовують ці приклади (рис. 2.3), необхідно зробити висновок про кілька кроків і фаз атаки.

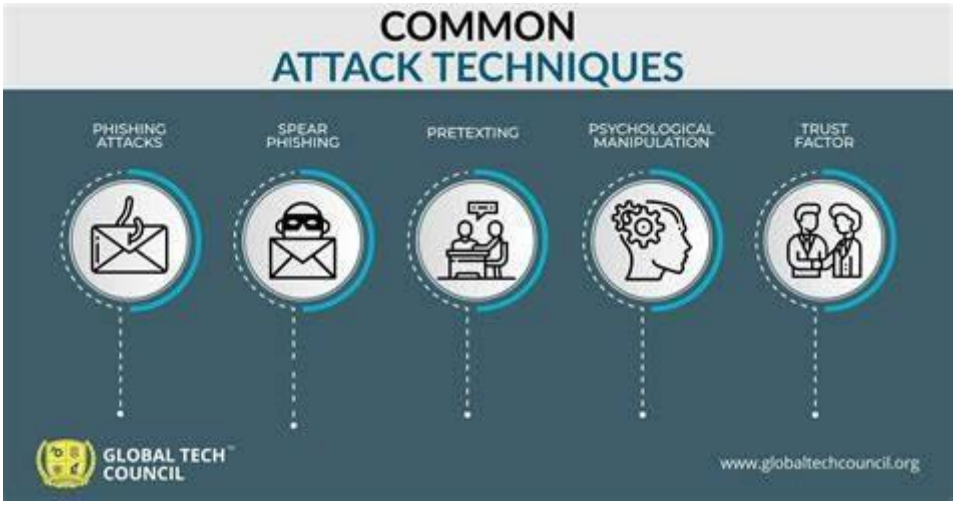

Рис. 2.3. Приклади атак соціальної інженерії

Дослідники також виявили, що атаки соціальної інженерії, які схожі з точки зору типу комунікації, засобу, мети, принципів і методів відповідності, мають схожий набір кроків і фаз (рис. 2.4) протягом усієї атаки соціальної інженерії.

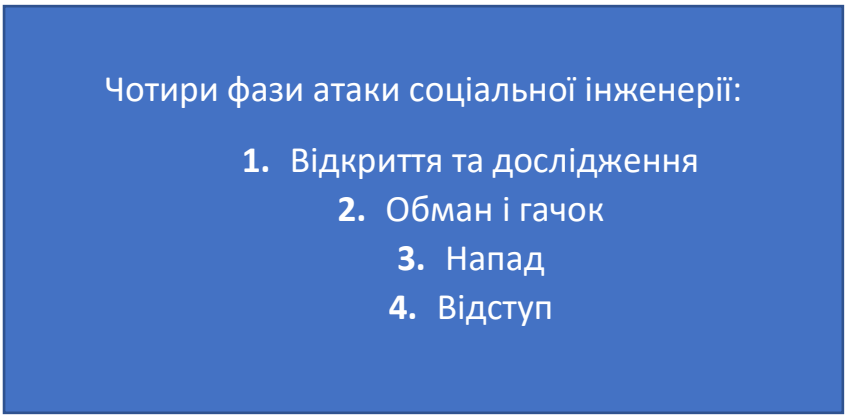

Рис. 2.4. Фази атак соціальної інженерії

Приклади атак соціальної інженерії, які мають схожий набір кроків і фаз, можуть бути згруповані разом, щоб сформувати шаблони атак соціальної

інженерії, які інкапсулюють детальний хід атаки, абстрагуючи об'єкти та об'єкти від атаки. Перевага групування подібних прикладів атак соціальної інженерії в шаблони атак соціальної інженерії полягає в тому, що один шаблон атаки соціальної інженерії може бути використаний для зображення декількох сценаріїв атак соціальної інженерії. Найпоширенішими атаками у 2024 році є (рис.2.5):

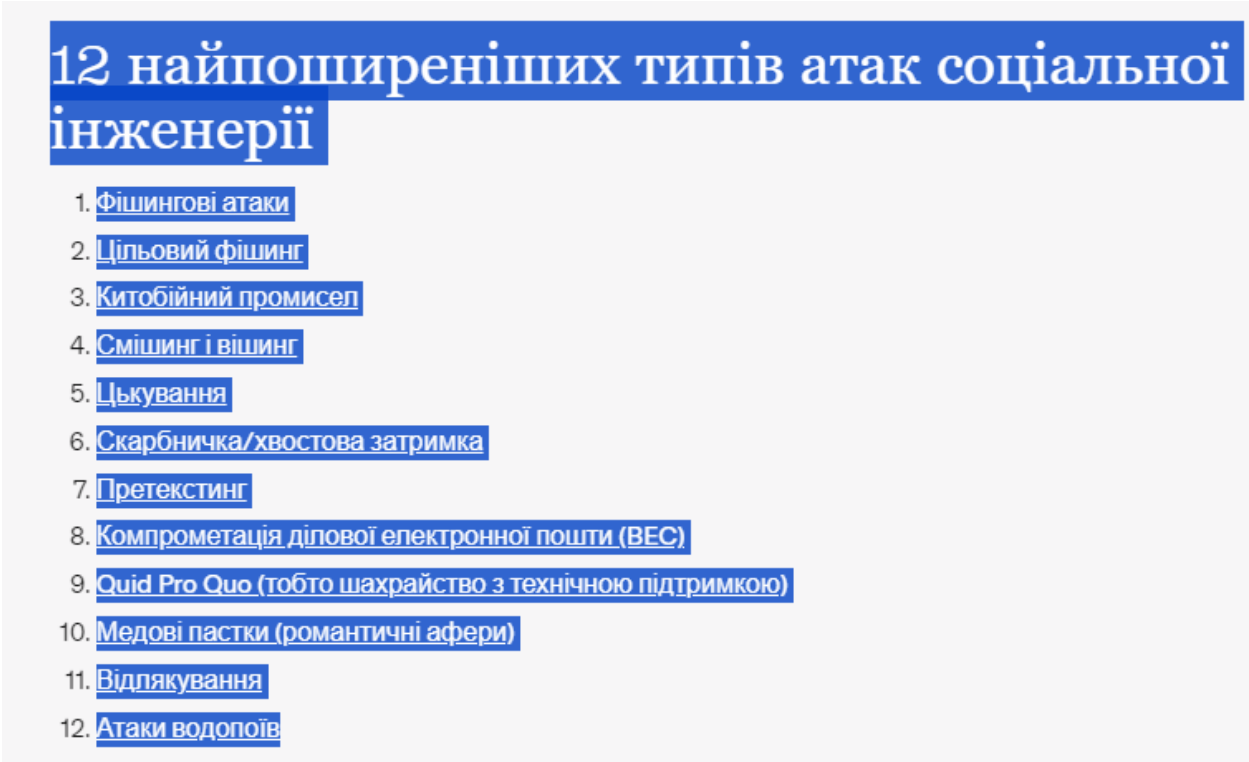

Рис. 2.5. 12 найпоширеніших атак у 2024 році

Для того, щоб порівнювати та перевіряти різні моделі, процеси та фреймворки в рамках соціальної інженерії, необхідно мати набір повністю деталізованих сценаріїв атак соціальної інженерії. Наявність набору шаблонів атак соціальної інженерії дозволить дослідникам тестувати свої моделі, процеси та фреймворки та порівнювати їх продуктивність з іншими моделями, процесами та фреймворками. У цьому документі пропонуються шаблони атак соціальної інженерії, які інкапсулюють кілька подібних прикладів атак соціальної інженерії в шаблони, які надають детальну інформацію про кожен крок і фазу атаки. Загальні шаблони містять опис атаки з детальним описом кожного кроку та фази атаки, а також список реальних прикладів атак соціальної інженерії, які можуть

бути зображені в шаблоні атаки соціальної інженерії. Кожен із шаблонів атак соціальної інженерії пояснюється зіставленням кожного кроку та фази шаблону з фреймворком атак соціальної інженерії.

Кіберзлочинці використовують різні тактики, щоб використовувати людську психологію та слабкі сторони, часто обходячи технічні заходи безпеки. У дослідженні [15] висвітлено кілька ключових типів атак соціальної інженерії:

- *фішинг*: шахраї надсилають шахрайські електронні листи або повідомлення, нібито з надійних джерел (наприклад, банків, компаній, колег), жертв обманом змушують розкрити конфіденційну інформацію або натиснути шкідливі посилання.
- *наманювання*: кіберзлочинці пропонують щось привабливе (наприклад, безкоштовне програмне забезпечення, знижки), щоб спонукати жертв завантажувати зловмисне програмне забезпечення або надавати особисті дані.
- *перетекст:* шахраї створюють сфабрикований сценарій (наприклад, видають себе за колегу чи авторитетну фігуру), щоб маніпулювати жертвами, щоб вони поділилися інформацією.
- *переслідування*: зловмисник фізично слідує за авторизованою особою в безпечну зону, прикидаючись частиною групи.
- *видача себе за іншу особу:* шахраї видають себе за іншу людину (наприклад, технічну підтримку, керівника компанії), щоб завоювати довіру та отримати інформацію.
- *експлуатація повноважень*: кіберзлочинці використовують свій уявний авторитет (наприклад, заявляючи, що належать до IRS), щоб маніпулювати жертвами.

2.2 Аналіз методів та технік соціальної інженерії

Незважаючи на технологічні вдосконалення інформаційної безпеки та постійні зусилля організацій щодо підвищення обізнаності користувачів про інформаційну безпеку, в останні роки атаки соціальної інженерії, зокрема, стають все більш серйозною загрозою для віртуальних спільнот. Згідно з останньою статистикою кібербезпеки, станом на перший квартал 2024 року на програмне забезпечення як послугу (SaaS) та веб-поштові сервіси організацій припадало 21 відсотка фішингових атак, при цьому найбільше атак припадало на соціальні мережі (рис. 2.6) [16].

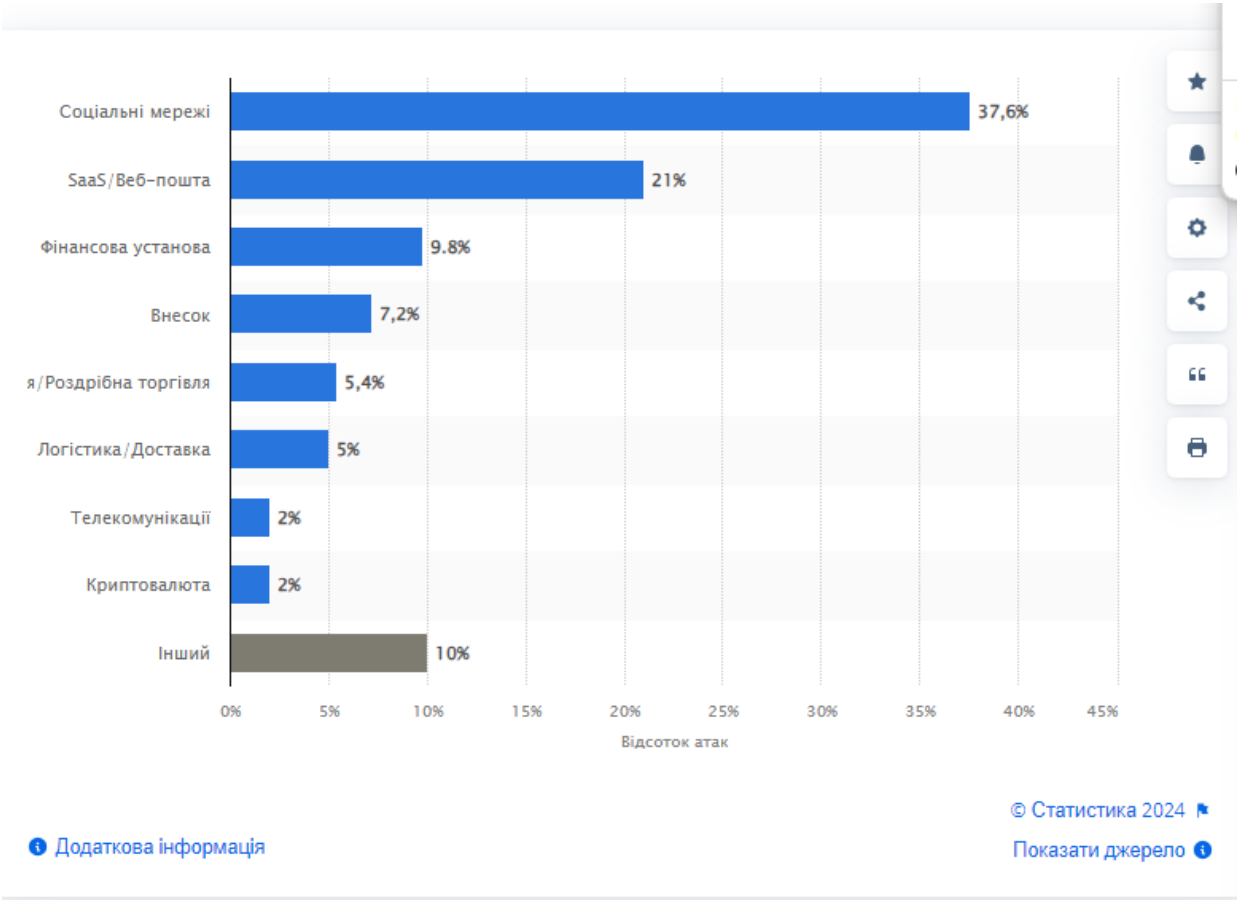

Рис. 2.6. Статистика атак соціальної інженерії

Близько 65 відсотків організацій стикалися з фішинговими атаками від однієї до п'ятдесяти на рік. Інший звіт показує, що інтернет-магазини є найбільш цілеспрямованими організаціями для фішингових атак. На жаль, сьогодні атаки соціальної інженерії, схоже, швидко послаблюють ланцюжок кібербезпеки а

соціальні інженери зловживають вразливостями безпеки в діловому та приватному середовищі для витоку конфіденційної інформації.

Нещодавні дослідження почали зосереджуватися на факторах, які змушують людей реагувати на фішингові атаки. У цьому дослідженні була проведена реальна цільова фішингова атака на співробітників в організаціях, щоб вивчити, як особистість користувачів, їх ставлення та сприйняті фактори ефективності впливають на їхню схильність піддаватися такій атаці. Цільові фішингові атаки є більш складними, ніж звичайні фішингові атаки, оскільки вони використовують особисту інформацію про передбачувану жертву та представляють серйознішу проблему для виявлення як потенційними жертвами, так і фішинговими фільтрами електронної пошти [17-19].

Фішинг є одним із найпопулярніших векторів кібератак загроза окремим особам, корпораціям та критичній інфраструктурі. Ці атаки призначені для того, щоб змусити користувачів подумати, що електронна пошта або веб-сайт є законними, і переконати їх розкрити імена користувачів і паролі або ненавмисно встановити зловмисне програмне забезпечення, натиснувши шкідливі посилання чи вкладення. Залежно від рівня обману, може бути важко автоматично перевіряти такі повідомлення. Як наслідок, людське судження відіграє важливу роль у всіх системах кібербезпеки і, за багатьма оцінками, є її найслабшою [20].

Визначення атак соціальної інженерії.

Тривіальний приклад атаки соціальної інженерії – це коли зловмисник хоче підключитися до мережі організації. В результаті своїх досліджень зловмисник з'ясовує, що співробітник служби підтримки знає пароль до бездротової мережі організації. Крім того, зловмисник отримав особисту інформацію про співробітника, якого ідентифікували як ціль. Зловмисник ініціює розмову з об'єктом, використовуючи отриману інформацію для встановлення довіри

Застосування шаблонів атак соціальної інженерії.

Шаблони атак соціальної інженерії були запропоновані з метою надати дослідникам набір шаблонів атак соціальної інженерії, які можуть бути використані для перевірки або порівняння інших моделей, процесів і

фреймворків в рамках соціальної інженерії. Кожен шаблон містив повний опис кожного етапу та пов'язаних з ним кроків фреймворку атак соціальної інженерії таким чином, що кожен шаблон надаватиме повторювані результати при використанні для перевірки або порівняння інших моделей [15, 21].

Основною загрозою інформаційній безпеці організації є зростання числа інцидентів, викликаних атаками соціальної інженерії. Класифікація атак показана на рисунку 2.7.

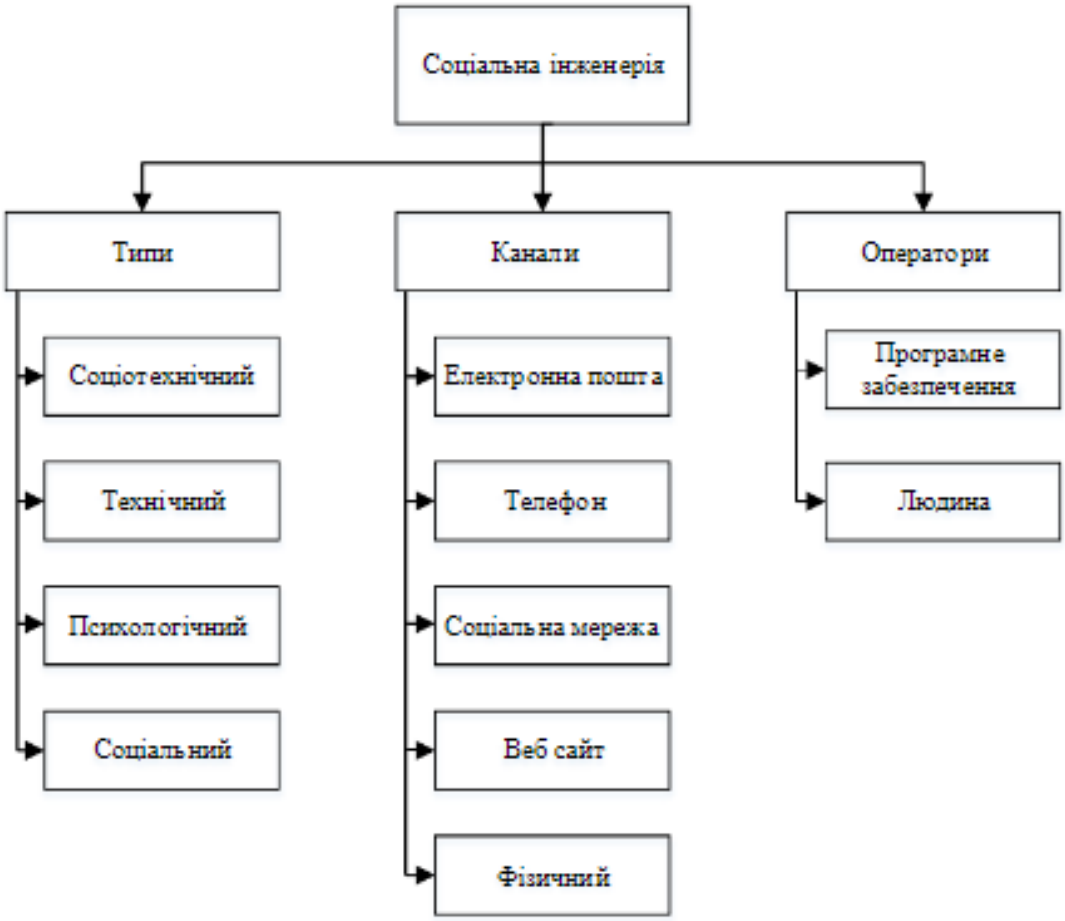

Рис. 2.7. Основні атаки соціальної інженерії

В комп’ютерному світі соціальна інженерія визначається як використання соціальних маскувань, культурних хитрощів і психологічних прийомів, щоб змусити користувачів комп'ютерів допомогти хакерам у незаконному вторгненні або використанні комп'ютерних систем і мереж [22]. Соціальна інженерія є однією з найпотужнішої зброї в арсеналі хакерів і авторів шкідливого коду,

оскільки набагато простіше обманом змусити когось дати свій пароль для системи, ніж витрачати зусилля на злом [23]. Незважаючи на постійні зусилля організацій щодо підвищення обізнаності користувачів про інформаційну безпеку, шкідливе програмне забезпечення соціальної інженерії успішно поширюється в Інтернеті та заражає численні комп'ютери. До 2007 року методи соціальної інженерії стали методом номер один, який використовується інсайдерами для скоєння електронних злочинів, але нічого не підозрюючі користувачі залишаються основним провідником для авторів шкідливого коду і по сьогоднішній день.

Враховуючи цю сприйнятливість до методів соціальної інженерії, основна мета досліджень науковців полягає у визначенні та описі тенденцій і тактик шкідливого програмного забезпечення соціальної інженерії.

Щоб шкідливе програмне забезпечення соціальної інженерії було успішним, воно має бути активоване кінцевим користувачем і безперебійно працювати в системі. Але якщо зловмисному програмному забезпеченню вдасться запобігти потраплянню до користувачів, воно не буде успішним. Визначення стратегій атак має життєво важливе значення для розробки контрзаходів, які можуть бути включені в превентивні механізми, такі як фільтрація електронної пошти та навчання безпеки кінцевих користувачів. Інформація про поведінку шкідливого програмного забезпечення під час його поширення допомагає у створенні систем раннього попередження. Навіть якщо зловмисне програмне забезпечення проходить етап запобігання та виконується користувачем, якщо його можна виявити на комп'ютері та заблокувати виконання шкідливої процедури, наслідки зловмисного програмного забезпечення можна пом'якшити [24].

Коли комп'ютерне шкідливе програмне забезпечення активовано, воно вносить різні зміни в комп'ютер, відкриваючи бекдори, які дозволяють йому поширюватися на інші комп'ютери. Він також застосовує захисні стратегії, щоб залишитися непоміченим. Виявлення таких захисних стратегій допомагає виявляти шкідливе програмне забезпечення на ранніх стадіях на машинах

кінцевих користувачів, а також блокувати його повне виконання та подальше поширення. Його виявлення також допомагає в розробці евристичного аналізу – методу сканування шкідливого програмного забезпечення, який оцінює патерни поведінки для виявлення аномалій. Дослідники безпеки використовують ці дані для побудови поведінкових моделей шкідливого програмного забезпечення, і кінцеві користувачі можуть отримувати сповіщення про незвичайну поведінку на своїх комп'ютерах.

Щоб надати рекомендації щодо посилення захисту організації від шкідливого програмного забезпечення соціальної інженерії, дослідники у своїх роботах [7, 21-24] зібрали дані про такі шкідливі програми та проаналізували їхні характеристики. Аналіз цих робіт дозволив визначити використовувані стратегії, як психологічні, так і технічні, емпіричні докази зростаючого охоплення шкідливого програмного забезпечення соціальної інженерії, описано процес збору даних і узагальнено тенденції інцидентів, пов'язаних із шкідливим програмним забезпеченням соціальної інженерії. Після представлення структури поширення шкідливого програмного забезпечення соціальної інженерії необхідно визначити деякі поширені шляхи атаки. Після цього визначення потрібно провести аналіз психологічної тактики, яку використовує зловмисне програмне забезпечення, а також описи деяких технічних функцій, які розроблені, щоб допомогти зловмисному програмному забезпеченню протистояти існуючим заходам безпеки.

2.3 Оцінка етичних наслідків атак та їх вплив на кібербезпеку організацій

Соціальна інженерія глибоко вкоренилася в галузях як інформатики, так і соціальної психології. Знання з обох цих дисциплін необхідні для проведення досліджень, заснованих на соціальній інженерії. При проведенні досліджень соціальної інженерії необхідно враховувати ряд етичних проблем і вимог, щоб

гарантувати, що шкода не спіткає тих, хто бере участь у таких дослідженнях. Ці побоювання і вимоги ще не формалізовані, і більшість дослідників не знають про етичні проблеми, пов'язані з дослідженнями соціальної інженерії.

У дослідженні [25] визначено низку проблем, пов'язаних із соціальною інженерією в публічній комунікації, тестуванням на проникнення та дослідженнями соціальної інженерії. Він також обговорює виявлені проблеми щодо трьох різних нормативно-етичних підходів (етика чесноти, утилітаризм і деонтологія) і наводить відповідні етичні перспективи, а також практичні приклади того, де ці формалізовані етичні проблеми для досліджень соціальної інженерії можуть бути корисними. У даній роботі пропонується етичний аналіз доброчесності соціальної інженерії в тестуванні на проникнення. Аналіз починається з розгляду попередніх досліджень на цю тему і стверджує, що такі спроби неправильно тлумачать або частіше ігнорують цю арістотелівську традицію. Він формулює основні принципи етики чеснот і застосовує їх до аналізу соціальної інженерії білих капелюхів. Аналіз етики доброчесності вимагає, щоб індивіди та фірми, які ініціюють тест на проникнення, були поміщені в ширший суспільний контекст, який зобов'язує осіб, які є потенційними жертвами людського злому, брати участь у створенні та процвітанні більших спільнот. Таким чином, для доброчесності етична згода не є необхідною умовою позитивного етичного статусу білої соціальної інженерії. Якщо методи узгоджуються з поміркованістю (тобто золотою серединою), маніпулювання нижчими рівнями в ієрархії спільнот може бути виправданим, якщо його можна розумно зрозуміти як частину зобов'язань щодо участі індивіда, і результати цієї участі є важливими для забезпечення евдемонії більшої спільноти. Тим не менш, золота середина вимагає, щоб надійні стратегії пом'якшення наслідків зменшували ступінь шкоди, заподіяної жертвам соціальної інженерії. Там, де це можливо, має бути досягнута певна згода в рамках цього пом'якшення. Нарешті, фірми, що проводять тестування на проникнення, повинні бути в змозі продемонструвати, що надійна програма етичної підготовки регулює використання соціальної інженерії.

Етика чесноти - це спосіб міркування з етичних питань, який розуміє етичну поведінку з точки зору звичок поведінки, які засвоюються і вбудовуються в соціальні відносини. Як традиція етичного міркування, етика чесноти почалася з Аристотеля, але за останні кілька десятиліть зазнала відродження в академічній філософії. Цей аргумент починається з розгляду попередніх досліджень етики соціальної інженерії і стверджує, що автори або неправильно витлумачили, або не помітили цю арістотелівську традицію. Потім він показує, як соціальна інженерія білих капелюхів найкраще розуміється за допомогою концепцій етики чесноти. Попередні етичні підходи ігнорують той факт, що особи, які беруть участь у тестуванні на проникнення, чи то піддослідні, чи самі хакери, повинні розглядатися в ширшому суспільному контексті, який зобов'язує жертв людського хакерства брати участь у створенні та процвітанні більших спільнот. Одним із результатів є те, що для етики доброчесності згода жертви не є необхідною умовою для соціальної інженерії білих капелюхів. Якщо методи узгоджуються з поміркованістю (тобто золотою серединою), то маніпуляції на нижчих рівнях в ієрархії спільнот є виправданими, якщо їх можна розумно розуміти як частину партисипативного зобов'язання індивіда перед спільнотами вищого порядку, і якщо результати цієї участі є важливими для забезпечення процвітання ширшої спільноти. Тим не менш, цей аргумент показує, що дотримання етичної поміркованості вимагає, щоб надійні стратегії пом'якшення наслідків, включаючи, де це можливо, ступінь згоди, зменшували ступінь шкоди, заподіяної жертвам соціальної інженерії. Нарешті, фірми, що проводять тестування на проникнення, повинні розробити надійну програму етичної підготовки, яка регулює використання соціальної інженері [26].

Висновки до розділу 2

Захист інформації є надзвичайно важливим у сучасному суспільстві, і навіть незважаючи на те, що рівень безпеки інформації постійно підвищується, єдиним слабким місцем залишається людина, яка схильна до методів маніпулювання. У поточній роботі розглядається соціальна інженерія як домен і

атаки соціальної інженерії як процес всередині цієї сфери.

Незважаючи на те, що комп'ютерні системи продовжують ставати більш безпечними завдяки кращій розробці та тестуванню програмного забезпечення, вони так само легко піддаються руйнуванню хакерами, які використовують методи соціальної інженерії. Ми визначили, що шкідливе програмне забезпечення соціальної інженерії є поширеним і постійним. Як представлено тут, наш аналіз стратегій атак показує, що атаки соціальної інженерії розвиваються і стають все більш складними та витонченими.

Розділ 3 РОЗРОБЛЕННЯ МЕТОДІВ ПРОТИДІЇ ВПЛИВУ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ НА ОРГАНІЗАЦІЙНУ КІБЕРБЕЗПЕКУ

3.1 Вибір технологій та інструментів реалізації

Для розробки методів протидії соціальній інженерії використовуються різні технології та інструменти, які допомагають ідентифікувати, запобігати та реагувати на такі атаки. Аналіз досліджень науковців [27-32] таких методів в науковій літературі дозволив їх згрупувати в таблиці 3.1.

Таблиця 3.1

Перелік технологій, інструментів для розробки методів протидії соціальній інженерії

Технології	Інструменти	Застосунки
Фільтрація та захист електронної пошти	Антифішингове програмне забезпечення	Proofpoint, Mimecast, Microsoft Defender for Office 365
	Спам-фільтри	SpamAssassin
Технології аутентифікації	Багатофакторна автентифікація (MFA)	Google Authenticator, Microsoft Authenticator
	Єдина точка входу (SSO)	Okta OneLogin
Навчання та підвищення обізнаності	Платформи навчання з кібербезпеки	KnowBe4 та PhishMe
	Інформативні матеріали	відео, інфографіка та посібники з безпеки
Моніторинг та аналіз	Системи виявлення та запобігання вторгнень (IDS/IPS)	Snort Suricata
	Моніторинг поведінки користувачів та аналітика (UEBA)	Splunk User Behavior Analytics (UBA) Exabeam
Інструменти управління доступом	Системи управління ідентифікацією та доступом (IAM)	SailPoint IBM Security Identity Governance and Intelligence
	Контроль доступу на основі ролей (RBAC)	політики доступу на основі ролей

Продовження таблиці 3.1

Технології	Інструменти	Застосунки
Інструменти для відстеження та реагування	Security Information and Event Management (SIEM)	Splunk, IBM QRadar або ArcSight
	Endpoint Detection and Response (EDR)	CrowdStrike Falcon Carbon Black
Захист веб-доступу	Web Application Firewalls (WAF)	Imperva або Cloudflare
	Content Filtering	інструменти для фільтрації веб-контенту Kidslox, Family Link
Аналітика та звітність	Платформи для звітності про інциденти	Service Desk ServiceNow
	Регулярний аудит безпеки	Nessus , OpenVAS
Кіберінтелект та аналітика загроз	Threat Intelligence Platforms (TIP)•	ThreatConnect або Recorded Future
	Аналіз даних про загрози:	Використання систем машинного навчання та великих даних для прогнозування та виявлення загроз.

Для фільтрації та захисту електронної пошти використовуються:

- антифішингове програмне забезпечення - інструменти, такі як Proofpoint, Mimecast, та Microsoft Defender for Office 365, які можуть виявляти та блокувати фішингові електронні листи;
- спам-фільтри - використання спам-фільтрів, таких як SpamAssassin, для блокування підозрілих повідомлень.

2. Для автентифікації застосовуються:

- багатофакторна автентифікація (MFA) - використання додаткових факторів автентифікації, таких як токени, мобільні додатки (наприклад, Google Authenticator, Microsoft Authenticator) або біометричні дані, для підвищення безпеки.
- єдина точка входу (SSO) - інструменти, такі як Okta або OneLogin, які спрощують процес входу та підвищують безпеку за рахунок централізованого управління доступом.

3. Навчання та підвищення обізнаності:

- платформи навчання з кібербезпеки - платформи, такі як KnowBe4 та

PhishMe, які пропонують інтерактивні курси, тренінги та симуляції атак для навчання працівників;

- інформативні матеріали - розробка та розповсюдження навчальних матеріалів, включаючи відео, інфографіку та посібники з безпеки.

4. Моніторинг та аналіз:

- системи виявлення та запобігання вторгнень (IDS/IPS) - інструменти, такі як Snort або Suricata, які аналізують мережевий трафік для виявлення підозрілих дій;
- моніторинг поведінки користувачів та аналітика (UEBA) - інструменти, такі як Splunk User Behavior Analytics (UBA) або Exabeam, які використовують машинне навчання для виявлення аномальної поведінки користувачів.

5. Інструменти управління доступом:

- системи управління ідентифікацією та доступом (IAM) - рішення, такі як SailPoint або IBM Security Identity Governance and Intelligence, які допомагають управляти доступом до ресурсів та забезпечують відповідність політикам безпеки;
- гонтроль доступу на основі ролей (RBAC) - впровадження політик доступу на основі ролей, щоб обмежити доступ до критичних ресурсів лише тим працівникам, які їх потребують.

6. Інструменти для відстеження та реагування:

- Security Information and Event Management (SIEM) - платформи, такі як Splunk, IBM QRadar або ArcSight, які збирають та аналізують дані про безпеку для виявлення та реагування на інциденти;
- Endpoint Detection and Response (EDR) - інструменти, такі як CrowdStrike Falcon або Carbon Black, які забезпечують захист кінцевих точок та можливість швидкого реагування на загрози.

7. Захист веб-доступу:

- Web Application Firewalls (WAF) - рішення, такі як Imperva або Cloudflare, які захищають веб-додатки від атак, включаючи соціальну інженерію через

веб-форми;

- Content Filtering - використання інструментів для фільтрації веб-контенту та блокування доступу до шкідливих сайтів.

8. Аналітика та звітність:

- платформи для звітності про інциденти: використання інструментів, таких як JIRA Service Desk або ServiceNow, для управління інцидентами та створення звітів про безпеку;
- регулярний аудит безпеки: проведення аудитів та пенет-тестів з використанням інструментів, таких як Nessus або OpenVAS, для оцінки вразливостей.

9. Кіберінтелект та аналітика загроз:

- Threat Intelligence Platforms (TIP) - інструменти, такі як ThreatConnect або Recorded Future, які надають інформацію про нові загрози та допомагають організаціям готуватися до можливих атак.
- аналіз даних про загрози - використання систем машинного навчання та великих даних для прогнозування та виявлення загроз.

Використання цих технологій та інструментів дозволяє організаціям створити багаторівневу систему захисту від атак соціальної інженерії, підвищити обізнаність працівників і забезпечити швидке реагування на інциденти.

В дослідженні [33] основну увагу приділено методу тестування на проникнення за допомогою інструментів Kali Linux, Social Engineering Defensive Framework, Social-Engineer Toolkit, Social Engineering Optimizer.

Враховуючи всі попередні дослідження, основні методи впливу, на які потрібно звертати особливу увагу фахівцю управління інформаційною та кібернетичною безпекою, їх цілі заходи і можна згрупувати, як показано на рисунку 3.1.

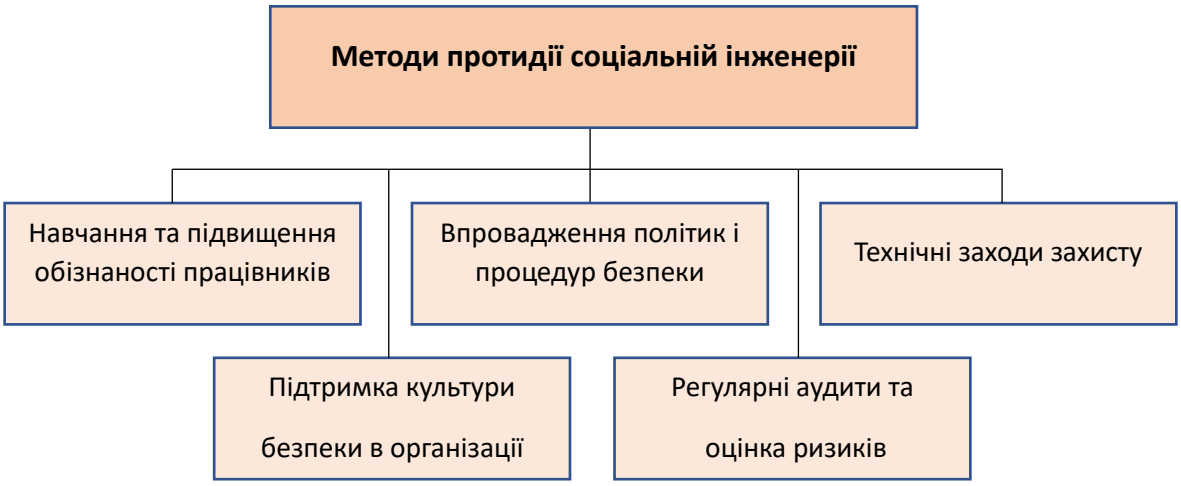

Рис. 3.1. Методи протидії впливу соціальній інженерії в організації

Детальний їх опис наступний:

1. Навчання та підвищення обізнаності працівників

Ціль: забезпечити всіх працівників знаннями про методи соціальної інженерії та навчити їх розпізнавати і правильно реагувати на можливі атаки.

Заходи:

- регулярні тренінги та семінари - організовувати щоквартальні тренінги для всіх працівників, на яких будуть розглядатися останні методи соціальної інженерії та способи захисту від них;
- імітаційні атаки - проводити регулярні імітаційні атаки (наприклад, фішингові кампанії) для перевірки готовності працівників та оцінки ефективності навчання;
- інформативні матеріали - розповсюджувати плакати, брошури та відео з інформацією про загрози соціальної інженерії та поради щодо безпеки;
- електронні курси - впровадити обов'язкові електронні курси з кібербезпеки для нових працівників та регулярні оновлювані курси для всіх працівників.

2. Впровадження політик і процедур безпеки

Ціль: забезпечити чіткі та зрозумілі інструкції для працівників щодо поведінки в ситуаціях, які можуть бути спровоковані атаками соціальної інженерії.

Заходи:

- розробка та впровадження політик - встановити політики, які регулюють обробку конфіденційної інформації, взаємодію з підозрілими запитами та правила використання корпоративних ресурсів;
- процедури реагування на інциденти - розробити чіткі інструкції для працівників щодо дій у разі підозри на атаку соціальної інженерії, включаючи контакти для повідомлення про інциденти;
- контроль доступу - встановити процедури контролю доступу до критично важливих ресурсів та інформації, включаючи багатофакторну автентифікацію.

3. Технічні заходи захисту

Ціль: Забезпечити захист інформаційних систем від атак соціальної інженерії за допомогою технічних рішень.

Заходи:

- встановити програмне забезпечення для фільтрації електронної пошти, виявлення та блокування фішингових листів та зловмисних вебсайтів;
- використовувати системи моніторингу мережевого трафіку та поведінки користувачів для виявлення підозрілих дій;
- оновлення та патчинг програмного забезпечення та застосовувати патчі безпеки для захисту від відомих вразливостей.

4. Культура безпеки в організації

Ціль: Створити культуру безпеки, де кожен працівник усвідомлює свою роль у захисті організаційної інформації.

Заходи:

- лідерство з боку керівництва - вищий менеджмент повинен демонструвати пріоритетність безпеки, підтримуючи всі ініціативи та політики;
- зворотний зв'язок - заохочувати працівників повідомляти про підозрілі дії та потенційні загрози, надавати анонімні канали для повідомлень;
- нагороди та визнання - впровадити систему нагород для працівників, які проявляють високу обізнаність та відповідальність у питаннях

кібербезпеки.

5. Регулярні аудити та оцінка ризиків

Ціль: Постійно оцінювати ефективність впроваджених заходів і виявляти нові потенційні загрози.

Заходи:

- аудити безпеки - проводити регулярні внутрішні та зовнішні аудити інформаційних систем і процедур безпеки;
- оцінка ризиків - регулярно оцінювати ризики, пов'язані з соціальною інженерією, та коригувати політики і процедури відповідно до нових загроз;
- звіти та аналітика - готувати регулярні звіти про стан безпеки та ефективність заходів протидії соціальній інженерії для керівництва.

Цей метод протидії соціальній інженерії допоможе значно підвищити рівень кібербезпеки в організації, зменшуючи ризики атак і покращуючи готовність працівників до захисту інформаційних ресурсів.

3.2 Розробка програмного забезпечення

Програмне забезпечення, яке застосовується для протидії впливу соціальної інженерії на організаційну безпеку, включає різноманітні інструменти для фільтрації, виявлення загроз, навчання працівників та управління доступом. Основні з них наведені в таблиці 3.1. Використання цих програмних рішень допомагає організаціям ефективно захищатися від атак соціальної інженерії, підвищуючи обізнаність працівників, запобігаючи фішинговим атакам та забезпечуючи надійний контроль доступу до критичних ресурсів.

Разом з тим, для автоматизації протидії впливу соціальній інженерії необхідно розробити комплексні рішення, які охоплюють різні аспекти кібербезпеки. Основні напрямки додаткових розробок наступні:

1. Інтеграція та автоматизація навчання:

- адаптивне навчання на основі ризиків - розробити систему, яка

автоматично налаштовує навчальні програми на основі індивідуальних ризиків та поведінки працівників. Наприклад, якщо хтось кілька разів став жертвою фішингових атак, ця система може автоматично призначати додаткові тренінги;

- гейміфікація - впровадити елементи гейміфікації в навчальні програми для підвищення зацікавленості та мотивації працівників.

2. Автоматичне виявлення та блокування загроз:

- машинне навчання та штучний інтелект - розробити моделі машинного навчання, які здатні виявляти підозрілу поведінку або аномалії в мережевому трафіку та електронній пошті, ці моделі можуть бути інтегровані з існуючими системами моніторингу безпеки.
- автоматизовані відповіді на інциденти (SOAR) - використання платформ Security Orchestration, Automation, and Response (SOAR), таких як Palo Alto Networks Cortex XSOAR або Splunk Phantom, для автоматизації процесів реагування на інциденти, це включає автоматичне блокування підозрілих облікових записів, ізоляцію пристроїв, які можуть бути скомпрометовані, і запуск додаткових перевірок.

3. Покращення засобів автентифікації:

- контекстуальна автентифікація - розробити системи, які враховують контекстні фактори під час автентифікації (наприклад, геолокацію, час доби, тип пристрою) і автоматично застосовують додаткові перевірки при виявленні аномалій;
- біометричні технології - інтеграція більш розвинених біометричних технологій, таких як розпізнавання обличчя, відбитків пальців або голосу, для підвищення рівня безпеки при автентифікації користувачів.

4. Розширений моніторинг та аналіз:

- аналітика поведінки користувачів (UBA/UEBA) - розробити більш точні та адаптивні системи для моніторингу та аналізу поведінки користувачів; це може включати створення профілів нормальної поведінки користувачів та автоматичне виявлення аномалій.

- реальний час аналітики загроз - розробити системи, які забезпечують аналіз загроз в реальному часі та автоматично оновлюють політики безпеки та контрзаходи.

5. Інтеграція та управління даними:

- централізоване управління загрозами - розробити інтегровану платформу, яка об'єднує дані з різних джерел (фільтрація електронної пошти, моніторинг мережі, дані про поведінку користувачів) та забезпечує єдину точку управління для всіх аспектів кібербезпеки;
- автоматизоване оновлення політик - системи, які автоматично оновлюють політики безпеки на основі останніх даних про загрози та вразливості.

6. Тестування та симуляція атак:

- імітація соціальної інженерії - розробити автоматизовані інструменти для симуляції атак соціальної інженерії, включаючи фішингові кампанії, щоб регулярно перевіряти готовність працівників та ефективність навчання;
- Red Team/Blue Team інструменти - інтеграція інструментів для червоних (атакуючих) та синіх (захисних) команд для тестування та покращення заходів безпеки.

7. Зворотний зв'язок та аналітика ефективності:

- системи зворотного зв'язку - розробка інструментів, які дозволяють працівникам надавати зворотний зв'язок щодо навчальних програм і симуляцій атак, що допоможе покращити їх ефективність;
- аналіз ефективності заходів - автоматизовані системи для аналізу ефективності впроваджених заходів та політик безпеки, які надають рекомендації для подальшого покращення.

Впровадження цих додаткових технологій та інструментів допоможе створити більш автоматизовану та ефективну систему протидії впливу соціальної інженерії, підвищивши загальний рівень кібербезпеки організації.

Python надає широкий спектр бібліотек та інструментів для розробки програм для автоматизації протидії соціальній інженерії. Ці приклади показують, як можна реалізувати різні аспекти кібербезпеки, такі як фішингові симуляції,

аналіз логів, багатофакторна автентифікація, моніторинг мережевого трафіку, автоматизація звітності та оновлення політик безпеки. Використовуючи ці підходи, можна значно підвищити рівень захисту організації від атак соціальної інженерії.

Розробка програм на Python для автоматизації протидії соціальній інженерії передбачає кілька етапів. Нижче наведено покроковий алгоритм (рис. 3.2), який допоможе структурувати цей процес.

Рис. 3.2. Алгоритм розроблення програми на Python

1. Визначення цілей і вимог

- ідентифікація проблеми - конкретні загрози соціальної інженерії, які автоматизувати (наприклад, фішинг, аналіз логів, навчання працівників);

- визначення функціональних та нефункціональних вимог до програми (наприклад, інтеграція з існуючими системами, обсяг даних для аналізу, вимоги до продуктивності).

2. Аналіз та проектування

- вибір технологій та інструментів - відповідні бібліотеки та фреймворки на Python (наприклад, *smtplib* для відправки електронних листів, *pandas* для аналізу даних, *pyotp* для двофакторної автентифікації);
- проектування архітектури системи , включаючи модулі та їх взаємодію;
- розробка алгоритмів, які будуть використовуватися для виявлення загроз, навчання працівників, аналізу логів тощо.

3. Розробка

- ініціалізація проекту, створення структури проекту та налаштування середовище розробки;
- реалізація функціоналу, розробка основних модулів програми, тестуючи кожен модуль окремо:
    - фішингові симуляції - написання скрипта для відправки фішингових електронних листів (Додаток А);
    - аналіз логів - реалізація обробки логів для виявлення аномальної поведінки(Додаток Б);
    - двофакторна автентифікація - додати функціонал для генерації та перевірки одноразових паролів (Додаток В);
    - моніторинг мережі і створення скрипта для моніторингу мережевого трафіку(Додаток Г);
    - автоматизація звітності і аналізу (Додаток Д);
    - автоматизація оновлення політик безпеки (Додаток Ж).
- інтеграція всіх модулів в єдину систему та забезпечення їх взаємодії.

4. Тестування

- юніт-тестування, розробка тестів для кожного модуля окремо, використовуючи бібліотеки, такі як *unittest або pytest*;

- інтеграційне тестування, перевірка взаємодії між модулями та їх сумісність;
- тестування на безпеку: на вразливості, щоб забезпечити безпеку програми.

5. Розгортання

- підготовка середовища для розгортання (сервери, бази даних, мережеві налаштування);
- розгортання програми на обраному середовищі;
- підготовка документації для користувачів та адміністраторів.

6. Моніторинг та підтримка

- моніторинг продуктивності, встановлення інструментів для моніторингу продуктивності та безпеки програми;
- оновлення та виправлення помилок;
- зворотній зв'язок: відгуки користувачів для покращення функціоналу програми.

Цей алгоритм і приклади коду в Додатках А-Ж допоможуть розробити ефективні програми для автоматизації протидії соціальній інженерії.

3.3 Тестування та налагодження програмного коду автоматизації

Фрагменти програмного коду були протестовані на навчальних даних. Для прикладу, код, наведений на рис.3.3 забезпечує автоматизацію обробки логфайлів із збереженою історією. Цей код виконує наступні дії:

1. Імпортує необхідні бібліотеки:
    - *pandas* для роботи з даними у форматі таблиць (DataFrame).
    - *pyplot* з бібліотеки `matplotlib` для створення графіків.
2. Функція *generate_report(log_file):*
    - читає файл журналу (лог-файл) у форматі CSV, який вказаний у параметрі *log_file*.

- створює звіт, який містить кількість записів для кожного типу активності у журналі.
- побудовує стовпчасту діаграму *(bar plot)* для візуалізації цього звіту;
- додає заголовок та підписи до осей графіка;
- зберігає графік у файл *activity_report.png*.

3. Виклик функції *generate_report("activity_logs.csv"):*
   - викликає функцію з файлом activity_logs.csv, в якому містяться дані журналу активності.

Результат виконання коду

Після виконання цього коду буде створено та збережено файл activity_report.png, який міститиме стовпчасту діаграму. Ця діаграма буде показувати кількість записів для кожного типу активності з файлу activity_logs.csv. Кожен стовпець на діаграмі буде відповідати конкретному типу активності, а висота стовпця - кількості випадків цієї активності у журналі.

```
mport pandas as pd from matplotlib
 import pyplot as plt
def generate_report(log_file):
        logs = pd.read_csv(log_file) report = logs['activity'].value_counts()
       report.plot(kind='bar') plt.title('Activity Report')
        plt.xlabel('Activity') plt.ylabel('Count')
       plt.savefig('activity_report.png')
generate_report("activity_logs.csv")
```

Рис. 3.3. Лістинг коду автоматизації обробки логфайлів

Для перевірки роботи коду створений логфайл наступного змісту (рис.3.4)

```
timestamp,activity
2024-06-01 12:00:00,login
2024-06-01 12:05:00,logout
2024-06-01 12:10:00,login
2024-06-01 12:15:00,download
2024-06-01 12:20:00,login
2024-06-01 12:25:00,login
2024-06-01 12:30:00,logout
2024-06-01 12:35:00,login
2024-06-01 12:40:00,download
2024-06-01 12:45:00,login
2024-06-01 12:50:00,login
2024-06-01 12:55:00,logout
2024-06-01 13:00:00,login
2024-06-01 13:05:00,download
2024-06-01 13:10:00,login"
```

Рис.3.4. Зміст логфайлу для контролю

Результат роботи фрагмента коду автоматизації обробки логфайлу показаний на рисунку 3.5.

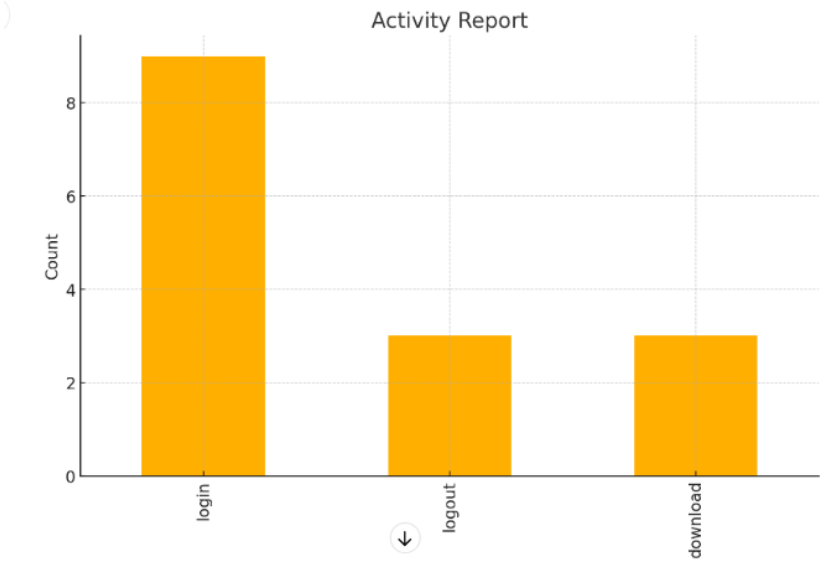

Рис. 3.5. Виведення результату автоматизованої обробки логфайлу

Графічна діаграма, створена за допомогою функції *pyplot* для даних з файлу "activity_logs.csv", виглядає так:

- заголовок діаграми: *Activity Report*
- ось X: Відображає різні типи активності (*login, logout, download*).
- ось Y: Відображає кількість кожного типу активності.

Значення на діаграмі (для контрольних даних):

- login: 9 разів
- logout: 3 рази
- download: 3 рази

Ця діаграма допомагає візуально оцінити, які типи активностей відбуваються найчастіше.

3.4 Рекомендації з практичного застосування

Практичне застосування наведених фрагментів програмного коду може значно підвищити рівень кіберзахисту в організаціях. Пропозиції щодо їх використання:

1. Фішингові симуляції

Мета: тренування працівників для розпізнавання фішингових атак і підвищення їх обізнаності щодо загроз соціальної інженерії.

Пропозиції:

- регулярне проведення фішингових симуляцій, автоматизація відправки фішингових листів на регулярній основі, щоб перевірити готовність працівників розпізнавати фішингові атаки;
- надавайте працівникам зворотний зв'язок і пояснення щодо того, як вони могли розпізнати фішингову атаку;

- відстежуйте та аналізуйте результати кожної симуляції для виявлення працівників або відділів, яким потрібні додаткові тренінги.

2. Аналіз логів та виявлення аномалій

Мета: виявлення підозрілої активності в логах для швидкого реагування на потенційні загрози.

Пропозиції:

- запровадьте автоматизований регулярний аналіз логів для виявлення аномалій або підозрілої активності;
- реагування на інциденти: встановіть автоматичні сповіщення або тригери для негайного реагування на виявлені загрози;
- генеруйте звіти на основі аналізу логів для керівництва та відповідальних за безпеку працівників.

3. Багатофакторна автентифікація (MFA)

Мета: посилення автентифікації користувачів для захисту критичних систем та даних.

Пропозиції:

- впровадження MFA для всіх критичних систем та облікових записів.
- використання біометричних методів для підвищення безпеки.

4. Моніторинг мережевого трафіку

*Мета:в*иявлення та запобігання підозрілої активності в мережі.

Пропозиції:

- моніторинг мережевого трафіку в реальному часі;
- використовуйте автоматизовані інструменти для швидкого автоматизованого реагування на підозрілу активність.

5. Автоматизація звітності та аналізу

*Мета: а*втоматизація процесу створення звітів для керівництва та підвищення прозорості безпекових процесів.

Пропозиції:

- налаштуйте автоматизоване створення звітів про активність та безпеку для регулярного перегляду керівництвом;

- використовуйте візуалізацію для кращого розуміння даних та швидкого прийняття рішень.

Висновки до розділу 3

Розробка та впровадження методів протидії соціальній інженерії є важливим кроком для підвищення рівня організаційної кібербезпеки. Використання сучасних технологій та інструментів дозволяє ефективно виявляти та запобігати атакам, підвищуючи захист інформаційних систем та зменшуючи ризики для організацій.

У розділі на етапі вибору технологій та інструментів реалізації було проведено детальний аналіз доступних рішень, що дозволяють ефективно протидіяти соціальній інженерії. Було обрано **Python** як основну мову програмування для розробки інструментів автоматизації, завдяки багатому набору бібліотек та широким можливостям для аналізу даних та мережевої безпеки. На основі обраних технологій було розроблено програмне забезпечення для автоматизації протидії соціальній інженерії, яке включало модуль для аналізу логів, модуль для фішингових симуляцій, модуль для багатофакторної автентифікації: Модуль для моніторингу мережевого трафіку. Розроблене програмне забезпечення було ретельно протестоване та налагоджене.

Розроблені методи та програмне забезпечення рекомендовано використовувати в організаціях для підвищення рівня кібербезпеки з наступними пропозиціями6 проводити симуляції на регулярній основі для підвищення обізнаності працівників щодо загроз соціальної інженерії; впровадити системи моніторингу логів та мережевого трафіку для своєчасного виявлення підозрілої активності; використовувати багатофакторну автентифікацію для захисту доступу до критичних систем; регулярно генерувати звіти про активність та стан безпеки для керівництва, щоб забезпечити прозорість та підвищити ефективність прийняття рішень.

Ці практичні рекомендації допоможуть організаціям ефективно використовувати наведенні фрагменти програмного коду для підвищення рівня кібербезпеки та захисту від загроз соціальної інженерії. Важливо регулярно переглядати та оновлювати ці інструменти, адаптуючись до нових загроз та технологій.

ВИСНОВКИ

Соціальна інженерія продовжує залишатися серйозною загрозою для організаційної кібербезпеки. Вивчення механізмів її впливу, розробка ефективних методів протидії та впровадження відповідних технологічних рішень є ключовими елементами для захисту організацій від подібних атак.

У роботі досліджено теоретичні основи, проаналізований вплив соціальної інженерії на організаційну кібербезпеку та розроблені методи протидії даній загрозі.

1. Проведений аналіз наукових праць і дослідження історії розвитку соціальної інженерії дозволив виявити еволюцію технік та методів, які використовуються для здійснення атак і залишаються сьогодні ефективним інструментом для кіберзлочинців. Аналіз встановив необхідність пошуку шляхів та наукових розробок удосконалення методів протидії впливу соціальної інженерії на організаційну кібербезпеку із застосуванням сучасних методик і інструментів.

2. Дослідження основних механізмів, через які соціальна інженерія впливає на кібербезпеку організацій, методів та технік соціальної інженерії дозволило виявити та сформувати реальні сценарії кібератак та встановити, як ці механізми працюють. За результатом розгляду етичних аспектів соціально-інженерних атак і їх впливу на працівників та загальну культуру безпеки в організаціях встановлено, що такі атаки можуть мати значні негативні наслідки, включаючи втрату довіри до внутрішніх систем безпеки та психологічний стрес для працівників.

3. Аналіз технологій та інструментів соціальної інженерії дозволив визначити методи протидії впливу соціальної інженерії на організаційну кібербезпеку, основними з яких є аналіз логів, моніторинг мережевого трафіку, фішингові симуляції та багатофакторна автентифікація, навчання персоналу.

4. З метою підвищення ефективності розроблено програмне забезпечення, яке включає інструменти для аналізу логів, генерації звітів та проведення фішингових симуляцій. Програмне забезпечення дозволяє

автоматизувати процеси захисту від соціальної інженерії та відрізняється від відомих тим, що враховує особливості кіберзахисту кожної організації при його впровадженні та налагодженні. Проведене тестування програмного забезпечення підтвердило його надійність та ефективність.

5. Надані практичні рекомендації щодо впровадження розроблених методів та програмного забезпечення в організаціях, які включають регулярне проведення фішингових симуляцій, моніторинг активності, використання багатофакторної автентифікації та автоматизоване створення звітів про безпеку.

Розроблені підходи та програмне забезпечення дозволяють підвищити рівень обізнаності працівників, покращити моніторинг та реагування на загрози, що в кінцевому рахунку сприяє зміцненню загальної кібербезпеки організацій. Проведене дослідження стало підґрунтям для створення ефективних стратегій захисту організацій від соціально-інженерних атак.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Hadnagy C. Social engineering: The art of human hacking. – John Wiley & Sons, 2010. 65 p.
2. Hatfield J. M. Social engineering in cybersecurity: The evolution of a concept. *Computers & Security*. 2018. Vol. 73. P. 102-113.
3. Steinmetz K.F., Pimentel, A., Goe, W.R. Decrypting Social Engineering: An Analysis of Conceptual Ambiguity. *Crit Crim*. 2020. № 28. P. 631–650. URL: https://doi.org/10.1007/s10612-019-09461-9. (date of access: 06.04.2024).
4. Bachmann M. Deciphering the hacker underground: First quantitative insights. Cyber Crime: Concepts, Methodologies, Tools and Applications. *IGI Global*. 2012. P. 175-194.
5. Brown Jr J. From Friday to Sunday: The hacker ethic and shifting notions of labour, leisure and intellectual property. *Leisure Studies*. 2008. Vol. 27. №. 4. P. 395-409.
6. Huseynov F., Ozdenizci Kose B. Using machine learning algorithms to predict individuals' tendency to be victim of social engineering attacks. *Information Development*. 2024. № 40(2), P. 298-318. https://doi.org/10.1177/02666669221116336. (date of access: 08.04.2024).
7. Krombholz K. Advanced social engineering attacks. *Journal of Information Security and applications*. 2015. Vol. 22. P. 113-122. URL: https://doi.org/10.1016/j.jisa.2014.09.005. (date of access: 08.04.2024).
8. Prabakaran M.K., Chandrasekar, A.D., MeenakshiSundaram, P. An enhanced deep learning-based phishing detection mechanism to effectively identify malicious urls using variational autoencoders. *IET Inf. Secur*. № 17(3) 2023. P. 423–440. URL: https://doi.org/10.1049/ise2.12106. (date of access: 09.04.2024).
9. Al Qahtani A.F., Cresci S. The covid-19 scamdemic: a survey of phishing attacks and their countermeasures during covid-19. *IET Inf. Secur*. № 16(5) 2022. P. 324–345. URL: https://doi.org/10.1049/ise2.12073. (date of access:

09.04.2024).

10. Calder Alan. Cyber Security: Essential Principles to Secure Your Organisation. *IT Governance Publishing*, 2020. *JSTOR.* P. 69 URL: https://doi.org/10.2307/j.ctv10crcbg. Accessed 2 June 2024. (date of access: 09.04.2024).
11. Про затвердження Положення про організаційно-технічну модель кіберзахисту: Постановка Кабінету Міністрів України від 29 грудня 2021 р. № 142, м Київ. URL: https://zakon.rada.gov.ua/laws/show/1426-2021-%D0%BF#Text (дата звернення 20.04.2024).
12. Wang Z., Zhu H., Sun L. Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods. *in IEEE Access*, 2021. vol. 9. P. 11895-11910. URL: https://doi.org 10.1109/ACCESS.2021.3051633. (date of access: 21.04.2024).
13. Francois Mouton, Louise Leenen, H.S. Venter, Social engineering attack examples, templates and scenarios. *Computers & Security*. 2016. Vol. 59. 2016. P. 186-209. URL: https://doi.org/10.1016/j.cose.2016.03.004. (date of access: 21.04.2024).
14. Mouton F., Leenen L., Venter H. S. Social engineering attack examples, templates and scenarios. *Computers & Security.* 2016. Vol. 59. P. 186-209. URL: https://doi.org/10.1016/j.cose.2016.03.004. (date of access: 21.04.2024).
15. Campbell C.C. Solutions for counteracting human deception in social engineering attacks. *Inf. Technol. People* 2019. № 32(5). P. 1130–1152. URL: https://doi.org/10.1108/itp-12-2017-0422. (date of access: 21.04.2024).
16. Halevi T., Memon N., Nov O. Spear-phishing in the wild: A real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks. *Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks (January 2, 2015).* URL: https://dx.doi.org/10.2139/ssrn.2544742. (date of access: 21.04.2024).
17. Broadhurst Roderic, Katie Skinner, Nick Sifniotis,Matamoros-Macias, Bryan and Ipsen, Yuguang, Phishing and Cybercrime Risks. *in a University Student*

Community May 9, 2018. URL: https://dx.doi.org/10.2139/ssrn.3176319. (date of access: 21.04.2024).

18. Marusenko, R., Sokolov, V., Buriachok, V. Experimental Evaluation of Phishing Attack on High School Students. *In: Hu, Z., Petoukhov, S., Dychka, I., He, M. (eds) Advances in Computer Science for Engineering and Education III. ICCSEEA 2020. Advances in Intelligent Systems and Computing*, vol 1247. *Springer, Cham*. URL: https://doi.org/10.1007/978-3-030-55506-1_59. (date of access: 25.04.2024).
19. Canfield I., Fischhoff B., Davis A. Quantifying Phishing Susceptibility for Detection and Behaviour Decisions. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, Vol. 58 , issue 8. p. 1158 – 1172 URL: https://doi.org/10.1177/0018720816665025. (date of access: 25.04.2024).
20. Shahrom, M.F., et al.: A pilot analysis of factors affecting defense against social engineering attacks in the armed forces environment. *Open International Journal of Informatics*. 2021. № 9(1). P. 53–64. URL: https://doi.org/10.11113/oiji2021.9n1.28. (date of access: 25.04.2024).
21. Engebretson P. The Basics of Hacking and Penetration Testing. thical Hacking and Penetration Testing Made Easy. 2013. 322 p. URL: https://doi.org/10.1016/C2013-0-00019-9. (date of access: 21.04.2024).
22. Mokhor V.V., Tsurkan O.V., Herasymov R.P., Tsurkan V.V. Information Security Assessment of Computer Systems by Socio-engineering Approach. *Selected Papers of the XVII International Scientific and Practical Conference "Information Technologies and Security*. Kyiv, 2017. P. 92-98. [Online]. Available URL: https://ceur-ws.org/Vol-2067/paper13.pdf. (Accessed on: 25. 04. 2024).
23. M. Edwards, R. Larson, B. Green, A. Rashid, and A. Baron, "Panning for gold: Automatically analyzing online social engineering attack surfaces", *Computers & Security*. 2017. vol. 69. P. 18-34. URL: https://doi.org/10.1016/j.cose.2016.12.013. (date of access: 11.05.2024).
24. Heartfield R., Loukas G. Detecting semantic social engineering attacks with the

weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework". *Computers & Security*. 2018. vol. 76. P. 101–127. URL: https://doi.org/10.1016/j.cose.2018.02.020. (date of access: 11.05.2024).

25. Francois Mouton, Mercia M. Malan, Kai K. Kimppa, H.S. Venter. Necessity for ethics in social engineering research, *Computers & Security*. 2015. Vol. 55. P. 114-127. https://doi.org/10.1016/j.cose.2015.09.001. (date of access: 11.05.2024).
26. Joseph M. Hatfield, Virtuous human hacking: The ethics of social engineering in penetration-testing, *Computers & Securit.,* 2019. Vol. 83. P. 354-366. URL: https://doi.org/10.1016/j.cose.2019.02.012. (date of access: 11.05.2024).
27. Salahdine F, Kaabouch N. Social engineering attacks: A survey. Future internet. 2019. Apr 2;11(4):89. URL: https://doi.org/10.3390/fi11040089. (date of access: 11.05.2024).
28. Li T., Wang X., Ni Y. Aligning social concerns with information system security: a fundamental ontology for social engineering. *Inf. Syst*. 2020. 104. P.1 01699. URL: https://doi.org/10.1016/j.is.2020.101699. (date of access: 11.05.2024).
29. Cullen A., Armitage, L. The social engineering attack spiral (seas). *In: 2016 International Conference on Cyber Security and Protection of Digital Services Cyber Security*. 2016. P. 1–6. IEEE.
30. Wang Z. Social engineering in cybersecurity: a domain ontology and knowledge graph application examples. *Cybersecurity*. 2021. № 4(1). P. 1–21. URL: https://doi.org/10.1186/s42400-021-00094-6. (date of access: 11.05.2024).
31. Schaab P., Beckers K., Pape S. Social engineering defence mechanisms and counteracting training strategies. *Inf. Comput. Secur*. 2017. № 25(2). P. 206–222. URL: https://doi.org/10.1108/ics-04-2017-0022. (date of access: 11.05.2024).
32. Yasin, A. Counteracting social engineering attacks. *Comput. Fraud Secur*. 2021(10). P. 15–19. URL: https://doi.org/10.1016/s1361-3723(21)00108-1. (date of access: 11.05.2024).

33. Цуркан О., Герасимов Р., Крук О. Методи протидії соціальній інженерії. *Збірник «Інформаційні технології та безпека»*. 2019. 7(2). P. 161–170. URL: https://doi.org/10.20535/2411-1031.2019.7.2.190563 (дата звернення 19.05.2024).
34. Krombholtz K., Hobel H., Huber M., Weippl E. Advanced social engineering attacks. *Journal of Information security and applications*. 2014. P. 1-10, URL: https://doi.org/10.1016/j.jisa.2014. 09.005. (date of access: 19.05.2024).
35. Asnar, Y. Organizational patterns for security and dependability: from design to application. *Int. J. Secure Softw. Eng. (IJSSE)*. 2011. № 2(3). P. 1–22. URL: https://doi.org/10.4018/jsse.2011070101. (date of access: 19.05.2024).

ДОДАТКИ

Додаток А

ЛІСТИНГ ПРОГРАМИ ФІШИНГОВОЇ СИМУЛЯЦІЇ

```
import smtplib
from email.mime.text import MIMEText
from email.mime.multipart import MIMEMultipart

def send_phishing_email(target_email, subject, body):
    sender_email = "your_email@example.com"
    password = "your_password"

    msg = MIMEMultipart()
    msg['From'] = sender_email
    msg['To'] = target_email
    msg['Subject'] = subject

    msg.attach(MIMEText(body, 'plain'))

    server = smtplib.SMTP('smtp.example.com', 587)
    server.starttls()
    server.login(sender_email, password)
    text = msg.as_string()
    server.sendmail(sender_email, target_email, text)
    server.quit()

send_phishing_email("target@example.com", "Important Update", "Please click on this link to update your information.")
```

Додаток Б

ЛІСТИНГ ПРОГРАМИ АНАЛІЗУ ЛОГІВ ДЛЯ ВИЯВЛЕННЯ АНОМАЛЬНОЇ ПОВЕДІНКИ

```
import pandas as pd

def analyze_logs(log_file):
    logs = pd.read_csv(log_file)
    anomalies = logs[logs['activity'].apply(is_suspicious)]
    return anomalies

def is_suspicious(activity):
    # Визначити критерії підозрілої активності
    if "suspicious_action" in activity:
        return True
    return False

anomalous_logs = analyze_logs("activity_logs.csv")
print(anomalous_logs)
```

Додаток В

ЛІСТИНГ ПРОГРАМИ БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ (MFA)

```
import pyotp
import qrcode

def generate_otp_secret():
    return pyotp.random_base32()

def generate_qr_code(secret, username):
    uri = pyotp.totp.TOTP(secret).provisioning_uri(name=username,
issuer_name="Your Service")
    img = qrcode.make(uri)
    img.save(f"{username}_qrcode.png")

def verify_otp(secret, otp):
    totp = pyotp.TOTP(secret)
    return totp.verify(otp)

secret = generate_otp_secret()
username = "user@example.com"
generate_qr_code(secret, username)
otp = input("Enter OTP: ")
if verify_otp(secret, otp):
    print("Verified")
else:
    print("Invalid OTP")
```

Додаток Г

ЛІСТИНГ ПРОГРАМИ МОНІТОРИНГУ МЕРЕЖЕВОГО ТРАФІКУ

```
from scapy.all import *


def monitor_traffic(packet):
    if packet.haslayer(TCP):
        ip_src = packet[IP].src
        ip_dst = packet[IP].dst
        tcp_dport = packet[TCP].dport
        tcp_sport = packet[TCP].sport
        print(f"IP src: {ip_src} -> IP dst: {ip_dst} | TCP sport: {tcp_sport} -> TCP dport: {tcp_dport}")


sniff(prn=monitor_traffic, filter="tcp", store=0)
```

Додаток Д

ЛІСТИНГ ПРОГРАМИ АВТОМАТИЗАЦІЇ ЗВІТНОСТІ ТА АНАЛІЗУ

```
import pandas as pd
from matplotlib import pyplot as plt

def generate_report(log_file):
    logs = pd.read_csv(log_file)
    report = logs['activity'].value_counts()
    report.plot(kind='bar')
    plt.title('Activity Report')
    plt.xlabel('Activity')
    plt.ylabel('Count')
    plt.savefig('activity_report.png')

generate_report("activity_logs.csv")
```

Додаток Ж

ЛІСТИНГ ПРОГРАМИ АВТОМАТИЗАЦІЇ ОНОВЛЕННЯ ПОЛІТИК БЕЗПЕКИ

```
import json

def update_security_policies(policy_file, new_policies):
    with open(policy_file, 'r') as file:
        policies = json.load(file)

    policies.update(new_policies)

    with open(policy_file, 'w') as file:
        json.dump(policies, file, indent=4)

new_policies = {
    "password_policy": {
        "min_length": 12,
        "require_special_char": True
    }
}

update_security_policies("security_policies.json", new_policies)
```